WELL, THAT ESCALATED QUICKLY: FROM PENNY-STEALING MALWARE TO MULTI-MILLION-DOLLAR HEISTS, A QUICK OVERVIEW OF THE BITCOIN BONANZA IN THE DIGITAL ERA

Santiago Pontiroli
Kaspersky Lab, Argentina

Email santiago.pontiroli@kaspersky.com

ABSTRACT

From the rise and demise of Silk Road to the current state of the cryptocurrency frenzy, we'll travel together on this journey of mysterious characters, million-dollar robberies and stealthy malware that will make you think twice before going online with your money.

In this presentation, we'll analyse the most interesting malware samples that target the popular bitcoin currency as well as some of the major events that have surrounded it during this past year. We'll investigate the flaws that have allowed several bad guys to steal more money than one could ever imagine, and look at how they did it without ever firing a gun or even stepping into a bank.

We'll round off with a look at some of the benefits that digital currencies offer to Latin American countries, and at the state of cryptocurrency-stealing malware both in the Latin American region and worldwide. Ranging from malicious PACs to botnets, we'll get our hands dirty with some interesting technical details and statistics.

Hold on to your seats, this is going to be one bumpy (but fun) crypto-ride, uncovering hidden Latin America's cybercriminal operations!

INTRODUCTION

It all started around 2009, when a mysterious character using the pseudonym Satoshi Nakamoto released his research about a peer-to-peer electronic cash system, now popularly known as bitcoin. It promised several advantages over current cash systems, but little did we know the kind of changes it would bring to our everyday lives and the global economy as a whole.

Like any currency, bitcoin can be used to purchase or sell goods, as a unit for value measurement or as value storage, which can be saved and spent at a future point in time. It's unclear what the stable (fair) value of the currency will be until it reaches its maximum at 21 million units – currently, there are around 12 million units in circulation. It may still be looked upon by some as 'play money', or reserved just for the geeky crowd, but bitcoin is changing the way we see digital currencies, and increasingly resembling an interesting large-scale economy experiment with real-life benefits and consequences.

Due to the fact that the bitcoin currency is not controlled by a central authority, but by its contributors, it has made some governments rather nervous, resulting in a heated debate about whether it should be regulated. However, regulation is not entirely feasible, given the initial design of the bitcoin currency and network. After 2010, Satoshi disappeared from the project he created without leaving a trace (or so he thought), resulting in many urban legends about his revolutionary invention and secretive identity. What we know for sure is that after many years, bitcoin is as strong as ever.

Digital currencies have many potential advantages when we compare them to their real-life counterparts. They're fast, taking only around ten minutes to verify a transaction, and cheap, liberating the user from the need to maintain or pay processing

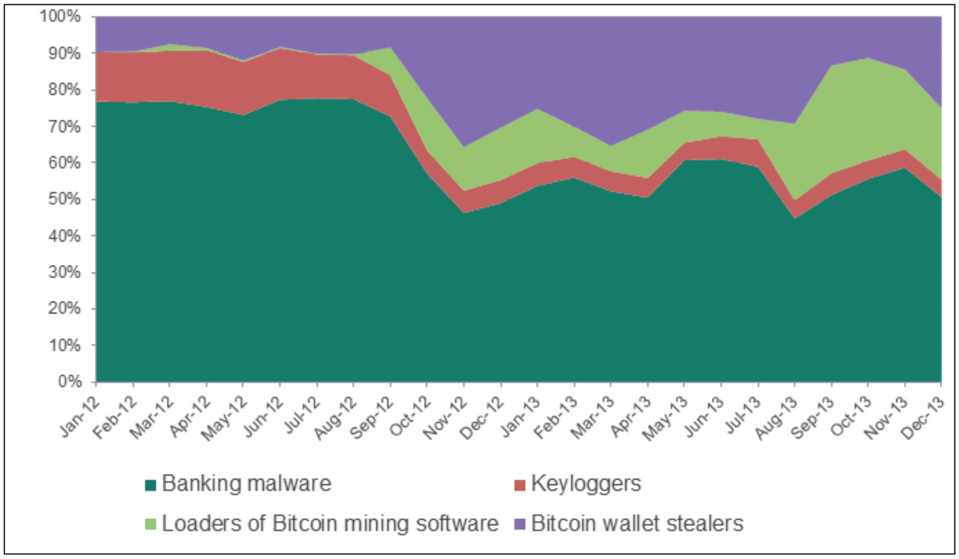


Figure 1: The percentage of users attacked by different types of malware each month [1].

fees to a credit card company. If we add the benefits of decentralization, privacy (not equal to anonymity) and ubiquity, we can begin to understand the temptation to invest time and money in bitcoins.

In some regions, especially Latin America, where the local currency suffers progressive and continuous devaluation, and the yearly inflation makes alternative currencies a viable and attractive option for saving your hard-earned salary, bitcoin is gaining momentum. In Argentina, an unofficial inflation rate of 25%, a 35% fee for credit card purchases in non-local currencies, and fears of another economic crash like the one in 2001, are forcing Argentinians to pay quite poor black market rates to get their hands on precious dollars or euros, albeit illegally. In the same way, the tech-savvy middle and upper classes are beginning to see bitcoin as a (legal) alternative to stashing American dollars.

> *'The most fertile ground for Bitcoin is in places like Cyprus, Argentina, Iceland, China and other countries which have experienced significant financial disruptions and/or maintain strict financial controls.'* – Garrick Hileman, economic historian at the London School of Economics.

While some early adopters have been involved in the bitcoin market from the beginning (by means of mining or simply by participating in exchanges), others are just grasping the concept of cryptocurrencies and learning about the perils of bitcoin by force – be it in the form of ransomware demanding a quick payment or malicious mining code consuming their limited computing resources. From wallet-stealing malware to large-scale bitcoin exchange heists, we can find just about anything in the crypto world, and this is just the beginning. Nowadays, we talk about malware and cybercrime as two sides of the same (bit)coin, usually referring to organized gangs of criminals with a clear differentiation of roles engaged in illegal activities with the sole purpose of financial profit. It makes sense, then, to observe a correlation in the number of malware samples targeting bitcoin users in the wild and the price of the currency being exchanged in markets worldwide.

FLAWS OF THE BITCOIN PROTOCOL

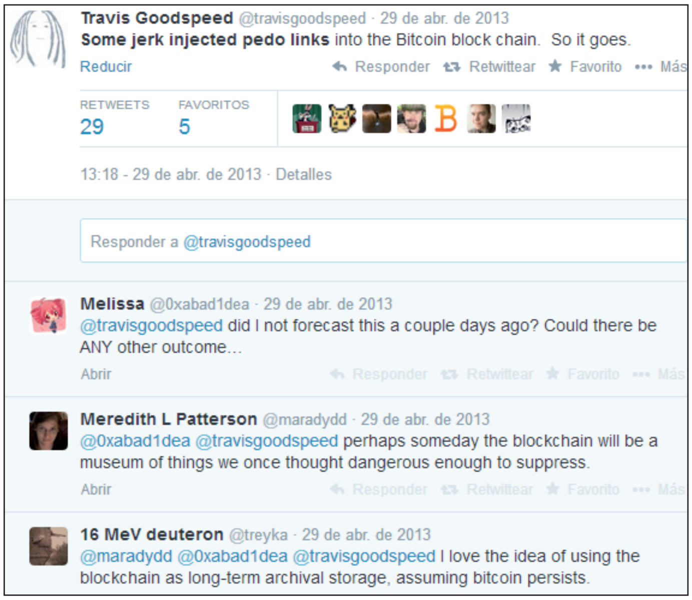
Transaction malleability

Made infamous by one of the (many) incidents suffered by the *Mt. Gox* exchange, transaction malleability is amongst the most common flaws discussed regarding the bitcoin protocol. However simple, and known about by the community since 2010, it has proven to be an effective method of attack in cases where one of the parties involved in the transaction is using a custom developed bitcoin wallet that doesn't take this flaw into consideration. The problem occurs due to the fact that the transaction ID (TXID) can be changed by a malicious node before the transaction is confirmed on the network. In this way, it can be made to appear as if the transaction didn't happen, forcing the sender to retry the operation (and in effect, withdrawing the funds once again).

As described in the research carried out by Christian Decker and Roger Wattenhofer, entitled 'Bitcoin Transaction Malleability and Mt. Gox' [2], there are very few indicators to suggest that transaction malleability was the sole cause of the demise of the popular bitcoin exchange. By analysing the incidents reported within the timeline in which they were made public, it seems that for the 850,000 bitcoins to disappear, a substantial number of transaction malleability attacks would have to have taken place in the network. Decker and Wattenhofer's research suggested that barely 386 bitcoins could have been stolen using malleability attacks – the difference is enough to blame bad business practices and not protocol flaws as the cause of *Mt. Gox*'s bankruptcy and missing funds.

Your PC is now stoned – illegal content in the blockchain

Although not entirely illegal, a curious piece of code was found within the bitcoin blockchain recently. *Microsoft*'s *Security Essentials* detected the signature of the STONED virus, popping up warnings about threats found inside the blockchain. This might be just an amusing anecdote now, but since the entire blockchain is downloaded for each client in order to be part of the network, we can wonder about the inclusion of illegal material there. Holding such material would be cause for prosecution in some countries, which is why a limitation on data storage in outbound transactions has been proposed [3].



Travis Goodspeed @travisgoodspeed · 29 de abr. de 2013
Some jerk injected pedo links into the Bitcoin block chain. So it goes.

RETWEETS 29 FAVORITOS 5

13:18 - 29 de abr. de 2013 · Detalles

Melissa @0xabad1dea · 29 de abr. de 2013
@travisgoodspeed did I not forecast this a couple days ago? Could there be ANY other outcome...

Meredith L Patterson @maradydd · 29 de abr. de 2013
@0xabad1dea @travisgoodspeed perhaps someday the blockchain will be a museum of things we once thought dangerous enough to suppress.

16 MeV deuteron @treyka · 29 de abr. de 2013
@maradydd @0xabad1dea @travisgoodspeed I love the idea of using the blockchain as long-term archival storage, assuming bitcoin persists.

Figure 2: Any content inserted in the blockchain will persist for the lifetime of the bitcoin network.

The 51% attack

If a single malicious entity were to control more than 50% of the network's mining hash rate, it would have full control of the bitcoin network and the possibility of manipulating the blockchain at will. Even though theoretically possible, the prohibitive cost of performing such an attack leaves well-funded agencies or governments that have massive computational power at their disposal as the only possible parties with the capability of engaging in this kind of network takeover.

Since bitcoin is considered a decentralized currency, there would be no single authority in charge of monitoring or stopping such an attack if it were to happen. Fortunately, it would be more profitable for an attacker simply to follow the rules of the network in order to maximize profits, instead of targeting their hashing power for malicious purposes. Conspiracy theories have been discussed, and the idea of someone pursuing this activity in order to create financial mayhem, causing bitcoin holders to lose confidence in the currency with a following rapid decline of the unit value is possible, but still highly unlikely to happen.

An attacker would be capable, for example, of reversing transactions sent by him or preventing other transactions from getting the confirmations needed to be added in the blockchain. It would still not be possible to reverse other people's transactions or prevent transactions from being sent at all. Modifications of the protocol itself still wouldn't be possible, and creating coins out of thin air or the attacker sending coins that never belonged to him is still out of scope [4].

A different scenario is presented when discussing mining pools. In the case of bitcoin, several months ago, the *Ghash.io* pool used by the cloud-hashing platform *Cex.io* was nearing 51% of the total bitcoin network hashrate. A great number of miners noticed this issue and changed pools immediately in order to avoid giving *Ghash.io* any more privileges over the network than it deserved. It is now considered good practice for mining pools to increase their fee when reaching the critical hashrate level so as to spread the miners (and their computing power) as evenly as possible.

Other cryptocurrencies have suffered the same ethical dilemma. *Coinotron* is a multi-coin mining pool [6]. The litecoin community noticed a combined hashrate of 51% for this pool and decided to take action in the same manner as seen in the bitcoin community. Currently, *Coinotron*'s hashrate is at around 38%, showing the preoccupation and involvement of the community in keeping their network from being controlled by a single entity.

One interesting aspect of the hashrate reported by most mining pools is that the Pareto principle still applies to the digital economy. In *Coinotron*, for example, 20 registered miners controlled approximately 37% of the network. This has more implications than may appear obvious – not only economical, but technological too. One cannot reach this level of processing power without resorting to ASICs and custom-built mining farms. Cryptocurrencies are no doubt theoretically decentralized, but the power is still in the hands of a few miners.

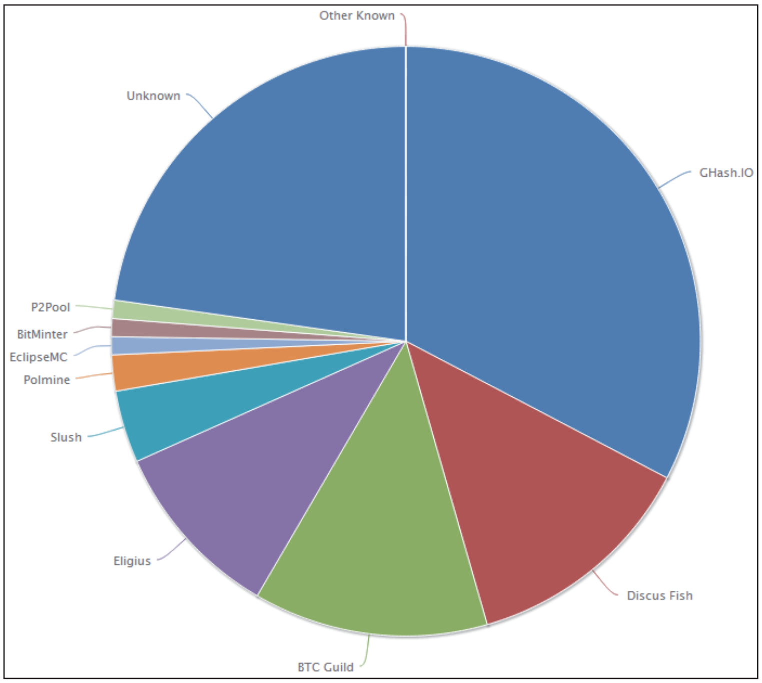


Figure 3: Distributed bitcoin network hashrate (as of 30 May 2014), sampling the last 30 days [5]. Currently displaying a combined computing hashrate of 82.19PH/s.

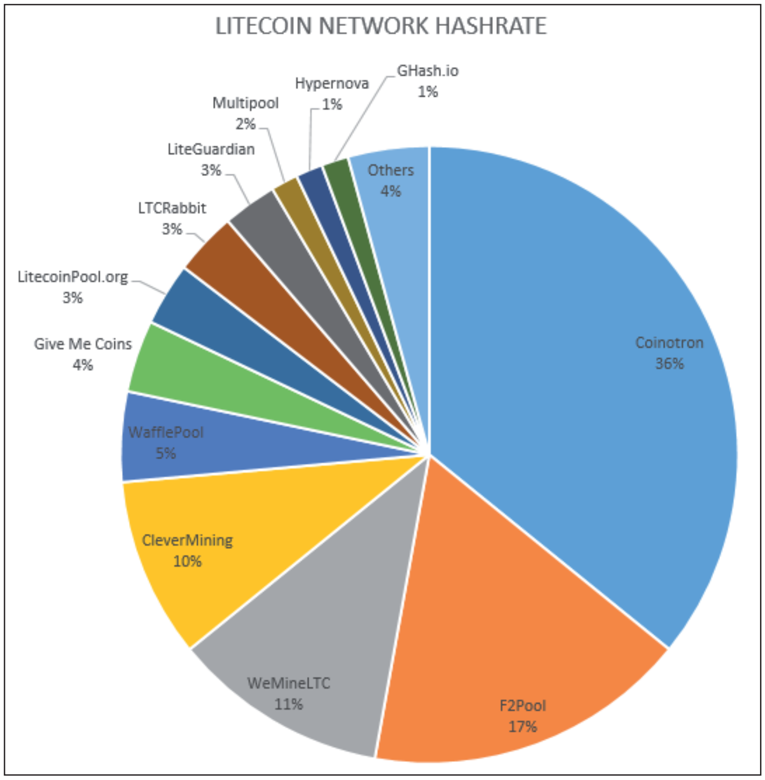


Figure 4: Distributed litecoin network hashrate as of 30 May 2014. The average total hashrate is approximately 281GH/s compared to the 40.615GH/s rate exhibited by the dogecoin scrypt-based mining network [7].

Denial of service

It is not only bitcoin exchanges that can be the target of massive distributed denial of service attacks [8], but also the network itself. While not affecting the funds of bitcoin users, these attacks prevent transactions from being confirmed, creating confusion in the network and aiding transaction malleability attacks. Even though bitcoin has some built-in protection against denial-of-service attacks, it has been found to be vulnerable to such types of attack (and will probably continue to be in the future).

Vulnerabilities

Like any other software, the 'Bitcoin Core' client has bugs and vulnerabilities which can be exploited. Analysing the CVE

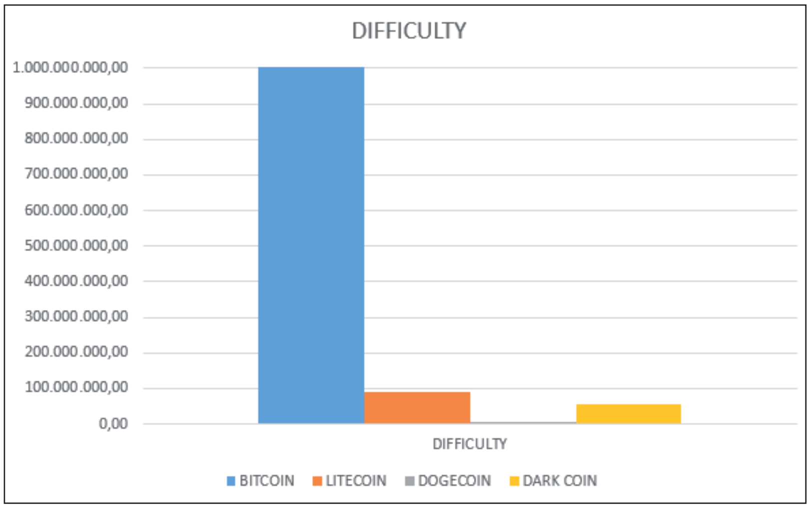
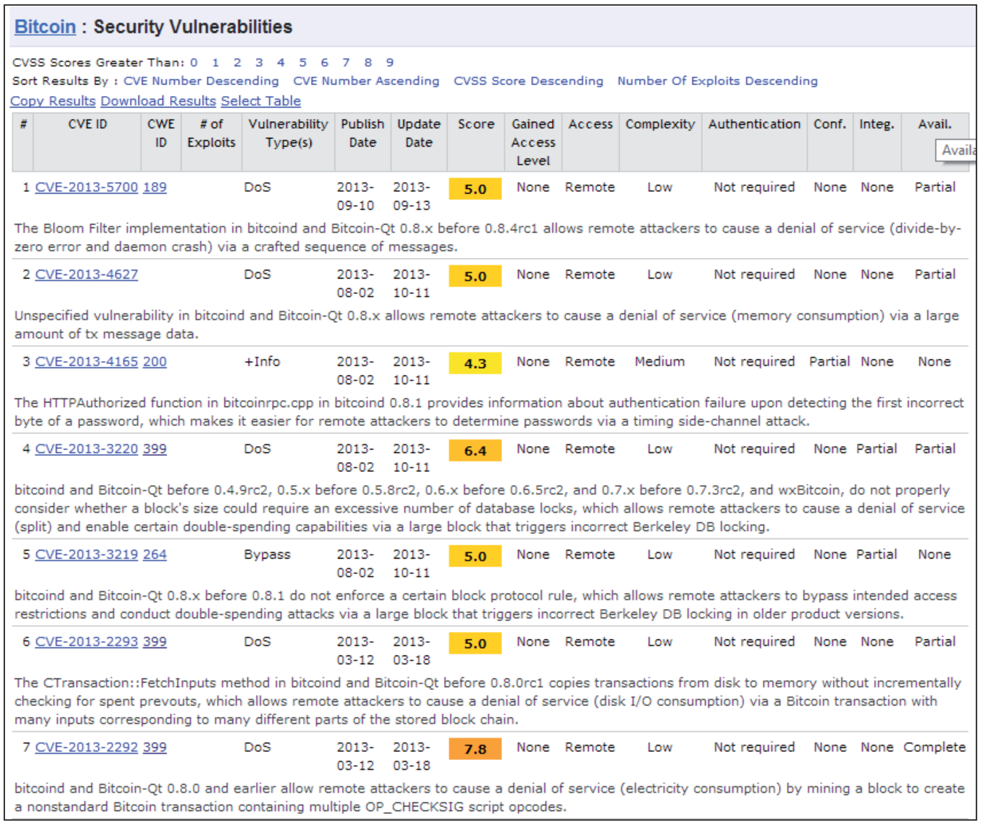


Figure 5: Comparison between the mining difficulty rates amongst the most popular cryptocurrencies.



Bitcoin : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results Select Table

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2013-5700</td><td>189</td><td></td><td>DoS</td><td>2013-09-10</td><td>2013-09-13</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">The Bloom Filter implementation in bitcoind and Bitcoin-Qt 0.8.x before 0.8.4rc1 allows remote attackers to cause a denial of service (divide-by-zero error and daemon crash) via a crafted sequence of messages.</td></tr>
<tr><td>2</td><td>CVE-2013-4627</td><td></td><td></td><td>DoS</td><td>2013-08-02</td><td>2013-10-11</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">Unspecified vulnerability in bitcoind and Bitcoin-Qt 0.8.x allows remote attackers to cause a denial of service (memory consumption) via a large amount of tx message data.</td></tr>
<tr><td>3</td><td>CVE-2013-4165</td><td>200</td><td></td><td>+Info</td><td>2013-08-02</td><td>2013-10-11</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Partial</td><td>None</td><td>None</td></tr>
<tr><td colspan="15">The HTTPAuthorized function in bitcoinrpc.cpp in bitcoind 0.8.1 provides information about authentication failure upon detecting the first incorrect byte of a password, which makes it easier for remote attackers to determine passwords via a timing side-channel attack.</td></tr>
<tr><td>4</td><td>CVE-2013-3220</td><td>399</td><td></td><td>DoS</td><td>2013-08-02</td><td>2013-10-11</td><td>6.4</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">bitcoind and Bitcoin-Qt before 0.4.9rc2, 0.5.x before 0.5.8rc2, 0.6.x before 0.6.5rc2, and 0.7.x before 0.7.3rc2, and wxBitcoin, do not properly consider whether a block's size could require an excessive number of database locks, which allows remote attackers to cause a denial of service (split) and enable certain double-spending capabilities via a large block that triggers incorrect Berkeley DB locking.</td></tr>
<tr><td>5</td><td>CVE-2013-3219</td><td>264</td><td></td><td>Bypass</td><td>2013-08-02</td><td>2013-10-11</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">bitcoind and Bitcoin-Qt 0.8.x before 0.8.1 do not enforce a certain block protocol rule, which allows remote attackers to bypass intended access restrictions and conduct double-spending attacks via a large block that triggers incorrect Berkeley DB locking in older product versions.</td></tr>
<tr><td>6</td><td>CVE-2013-2293</td><td>399</td><td></td><td>DoS</td><td>2013-03-12</td><td>2013-03-18</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">The CTransaction::FetchInputs method in bitcoind and Bitcoin-Qt before 0.8.0rc1 copies transactions from disk to memory without incrementally checking for spent prevouts, which allows remote attackers to cause a denial of service (disk I/O consumption) via a Bitcoin transaction with many inputs corresponding to many different parts of the stored block chain.</td></tr>
<tr><td>7</td><td>CVE-2013-2292</td><td>399</td><td></td><td>DoS</td><td>2013-03-12</td><td>2013-03-18</td><td>7.8</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Complete</td></tr>
<tr><td colspan="15">bitcoind and Bitcoin-Qt 0.8.0 and earlier allow remote attackers to cause a denial of service (electricity consumption) by mining a block to create a nonstandard Bitcoin transaction containing multiple OP_CHECKSIG script opcodes.</td></tr>
</table>

Figure 6: CVE details datasource query for bitcoin software and protocol-related vulnerabilities, displaying a predominance of DoS vulnerability type [10].

database, we can see that most of the vulnerabilities are denial-of-service-related. In spite of this, even the Heartbleed vulnerability [9] took the bitcoin world by surprise. Even though a fix was quickly released in version 0.9.1, and exchanges adopted the patch as soon as it was made available, this demonstrated how even a crypto bug in a related project (OpenSSL) could impact the security of the client, and the bitcoin unit value.

Anything else?

It's no wonder that cybercriminals see cryptocurrencies as a golden opportunity, with phishing scams relying on social engineering and bitcoin-stealing malware being common denominators in today's digital economy. The increase in bitcoin-related malware goes hand in hand with the increase in the currency's value, giving the phrase 'following the money trail' a whole new meaning.

As in the rest of the malware world, most of the bitcoin-related malware samples found target the *Windows* operating system, with very few of them targeting *Mac OSX* or *Linux*. In the mobile world, *Android* has the virtual monopoly on bitcoin-related infections, be they wallet stealers or even mining applications. As we have seen, there are many intrinsic flaws with the bitcoin protocol, although PEBKAC (problem exists between keyboard and chair) still holds true and users are the most common target for cybercriminals.

Losing the key to the wallet in which bitcoins are stored is a common problem in the bitcoin community, leaving any amount of savings locked up, and creating 'idle' coins which won't be able to used in the future.

Money laundering or 'bitwashing', mining botnets and the use of bitcoins to purchase illegal goods and services are just some of the issues that can't be categorized quite as easily. With currency exchanges headlining in newspapers around the world pretty much every week, it's difficult to blindly trust bitcoin, but after all of the incidents witnessed, we are now seeing a new generation of exchanges, with better business practices and, one can only hope, better security.

CRYPTOPOCALYPSE NOW – HISTORY OF BITCOIN EXCHANGE INCIDENTS

For quite some time, not a single week has gone by without one of the major bitcoin exchanges reaching mainstream news. We can attribute the success of some attacks to faulty technical implementations of the bitcoin wallet, others to clever social engineering approaches, and the rest to bad business practices and simple failure to adhere to proven security standards. There are too many incidents to list them all, but a handful of the most prominent ones are detailed in the paragraphs that follow. They all make great learning tools for the new generation of bitcoin exchanges.

Flexcoin, described as the 'world's first bitcoin bank' had its online storage stolen on 2 March 2014, with 896 bitcoins disappearing from 'hot wallets' in this single incident. Without ever firing a single gunshot, attackers demonstrated that we had already entered a new era of bank robberies. The loot of around 600,000 USD was enough to demonstrate the importance of the crypto market and highlight the lack of security measures taken by most of the exchange houses in the business. Stopping all transactions and shutting down the service was the first step to be taken after the rest of the common procedures for handling these situations. Unlike fiat currency handling banks, where insurance policies are in place, here there wasn't anyone to cover the losses, and the only way to resolve the issue was to return the funds present in cold storage and declare the end of the service.

In the same weekend, *Poloniex* announced a minor but crucial software bug that would ultimately decide the fate of this digital currency exchange business. On 4 March 2014, *Poloniex* owner Tristan D'Agosta announced on the *Bitcoin Talk* forum that the service had been hacked due to a bad implementation of the method in charge of checking the balance for all transactions the site handled. Apparently, the service allowed multiple withdrawals to be made without the software being able to check quickly enough for negative balances, leaving the possibility of stealing funds from the site's pool. As a result of not being able to cover the losses, the owner decided to deduct 12.3% from all accounts present on the site at that moment in order to keep on functioning.

On 14 March 2014, *Bitcurex* was on the front page of every major bitcoin news site, claiming that 10% to 20% of the funds present in its 'hot wallet' system had been stolen. As with other services, shutting down the website and halting transactions was the first measure taken – before even announcing that anything had gone wrong, leaving many users wondering what had happened to their money. Not long afterwards, *Bitcurex* announced through its website that it would resume operations on 18 March, and that, due to good monitoring practices, only part of the funds present in its system had been stolen, preventing a larger attack from happening.

Picostocks, which according to its official description facilitates valuation and fundraising for high-tech startup projects and companies and offers services for both bitcoin investors and entrepreneurs, lost 5,896 bitcoins on 29 November 2013. It had both its hot and cold wallet systems hacked, losing enough funds to raise suspicion of an 'inside job' from the bitcoin community.

A quarter-million-dollar heist is not something to frown upon, given the circumstances in which the following robbery took place. By accessing an unencrypted backup set of keys used for the *Bitfloor* exchange's wallet, the robbers had the keys to the kingdom to do their ill deeds at will. As with other exchanges, *Bitfloor* ceased all trading operations and promised to repay its customers. This demonstrated the instability and vulnerability of the bitcoin exchange industry as much as any of the other infamous cases. At a market value of 10.40 USD per unit, getting 250,000 USD for finding the keys to the vault seems like a good pay day for any cybercriminal. *Bitfloor* was the fourth bitcoin-based exchange, closely behind *Mt. Gox*, *BTC-E* and *Bitstamp*, but it was no stranger to similar incidents, having lost 25,000 user coins in 2012.

During its period of activity in 2011–2012, *Bitcoin Savings and Trust* showed the world that Ponzi schemes could also exist in a

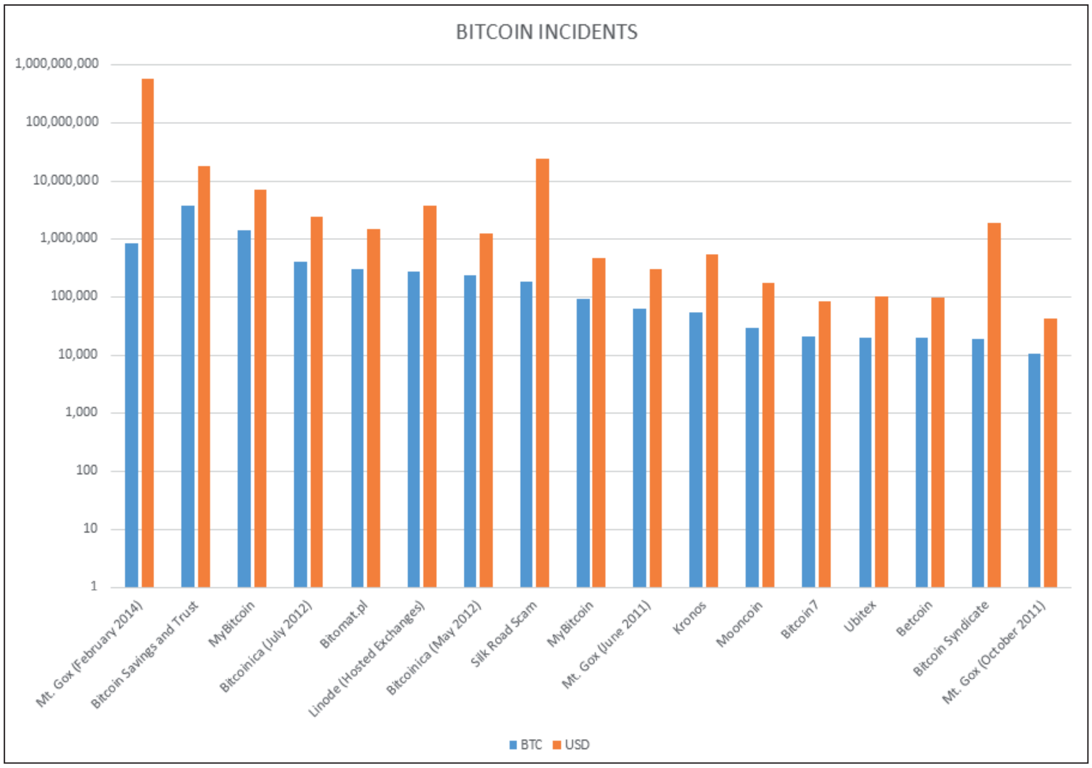


Figure 7: List of bitcoin heists with the most media coverage [11] shown in a logarithmic scale. Values taken from approximate historical BTC prices [12].

digital currency scenario. With 3,700 bitcoins stolen, this financial fraud, courtesy of Trendon T. Shavers, came as little shock to anyone. Owner of a service previously known as 'First Pirate Savings and Trust', Trendon (known online as 'pirateat40') was a Texan investor who promised weekly returns of 7% for your investment. The US Securities and Exchange Commission (SEC) called a halt to this operation, and the 'Bernie Madoff of bitcoin' had to cease his activities and face the music.

On 1 October 2013, *Canadian Bitcoins* entered the hall of fame for the silliest heist made on a bitcoin exchange. With nothing more than a chat session and smooth talk, a crafty cybercriminal convinced an attendee at *Rogers Data Centre* to reboot the *Canadian Bitcoins* server in fail safe mode, bypassing all security measures. Obtaining 149 bitcoins (worth 100,000 USD at the time) from hot wallet storage was the end result of this 'hack'. James Grant, the owner of *Canadian Bitcoins*, was puzzled to say the least, but still managed to cover the losses from his own pocket.

Bitcoinica witnessed two attacks during 2012 – one in July and one in May – setting a precedent in the local courts as the second case involving bitcoin to be filed in the legal system. Four users registered a complaint, asking to be compensated with 460,000 USD for the funds lost and grievance suffered. Even though at the time, the 18,547 bitcoins stolen were worth 90,000 USD, it made sense for the users to ask for a substantially higher compensation, given the ever-changing value of bitcoin.

Inputs.io's owner, ironically named 'TradeFortress', gave the bitcoin community an important security lesson after losing 4,100 BTC (1.2 million USD), stating: 'I don't recommend storing any bitcoins accessible on computers connected to the Internet'. Talk about bad timing: by 23 October 2013, these bitcoins were in the possession of a social engineer who managed to bypass the two-factor authentication used by the server hosted on the *Linode* cloud-hosting platform. The attacker compromised several mail accounts and finally was able to reset the server's master password.

Mt. Gox declares bankruptcy

The famous *Mt. Gox* exchange deserves a section of its own. The first reported incident involved a rogue Hong Kong IP address compromising one of the site's accounts, making a massive bitcoin sale and causing a frantic price drop. The attacker didn't profit much from this exploit, but confidence in the currency was tainted.

It wasn't until 24–26 February 2014 that *Mt. Gox* decided to close its doors, amidst allegations of a transaction malleability attack that had taken place – and gone unnoticed – over a long period of time. Criminals had stolen the shockingly high amount of 850,000 BTC (around of 7% of all bitcoins in existence and the equivalent of almost half a billion USD), leaving bitcoin enthusiasts venting their anger on forums, but with not much else to do in regards to restoring their funds. It's worth noting that, at one point, *Mt. Gox* handled more than 80% of trades in

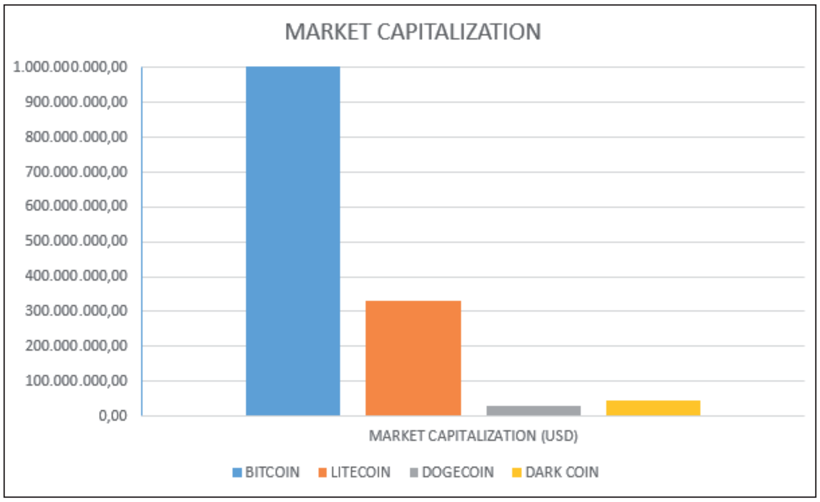


Figure 8: Market capitalization in USD as of 30 May 2014.

the virtual currency, being essentially no more than a single-man operation.

OTHER COINS

Although litecoin (LTC) resembles its big brother bitcoin in many ways, such as being an open-source peer-to-peer decentralized currency, the lead development team claims that 'litecoin is a proven medium of commerce complementary to bitcoin'. With a maximum supply limit of four times the one established for bitcoin (84 million units for LTC), it's amongst the most heavily traded alternative cryptocurrencies that fall under the deflationary category umbrella.

Introduced in October 2011, the limited geometric release of new coins and the controlled difficulty rate set at every 2,016 new blocks produced, makes litecoin the second largest cryptocurrency measured by market capitalization. In addition, as an intended improvement on the most noticeable bitcoin flaws, litecoin uses a scrypt proof-of-work algorithm in contrast to the SHA256 used by bitcoin, with the hopes of slowing down the creation of FPGA and ASIC mining farms. Processing each block takes 2.5 minutes, making it more suitable for fast transactions, compared to the 10 minutes required by bitcoin.

Based on a popular Internet meme, dogecoin (DOGE) has also become a big player in the cryptocurrency market. The greatly supportive community, fond of giving away DOGE tips and starting fundraisers for a variety of causes, has received enough media attention to make it interesting for cybercriminals. Beginning in December 2013, the DOGE founders didn't expect that a currency which used a Shiba Inu Japanese dog as its official logo would actually reach the levels currently seen. Being a controlled inflationary currency, there are expected to be 100 billion DOGE in circulation by the end of 2014, with 5.2 billion units released every year thereafter.

With the initial intention of reaching a broader audience, and with transaction confirmations taking as little as one minute, it has established itself as a showcase of how simple it is to start a new cryptocurrency trend. ATMs are already being manufactured, and the unorthodox and grammatically incorrect cryptocurrency has already sponsored a NASCAR driver, the Jamaican Bobsled Olympic team in Sochi, and several other charity-related activities. By also using scrypt technology in its proof-of-work algorithm, the developers make it clear that this is a currency that aims for fairness amongst participants.

But dogecoin wasn't the only currency that started as an internal joke. Coinye (COINYE), which faced a strong enough law suit to be put out of the market, was charged for copyright infringement of hip hop artist Kanye West's brand. Also scrypt based, and with a limit of 133,333,333,333 coins, the developers were clearly

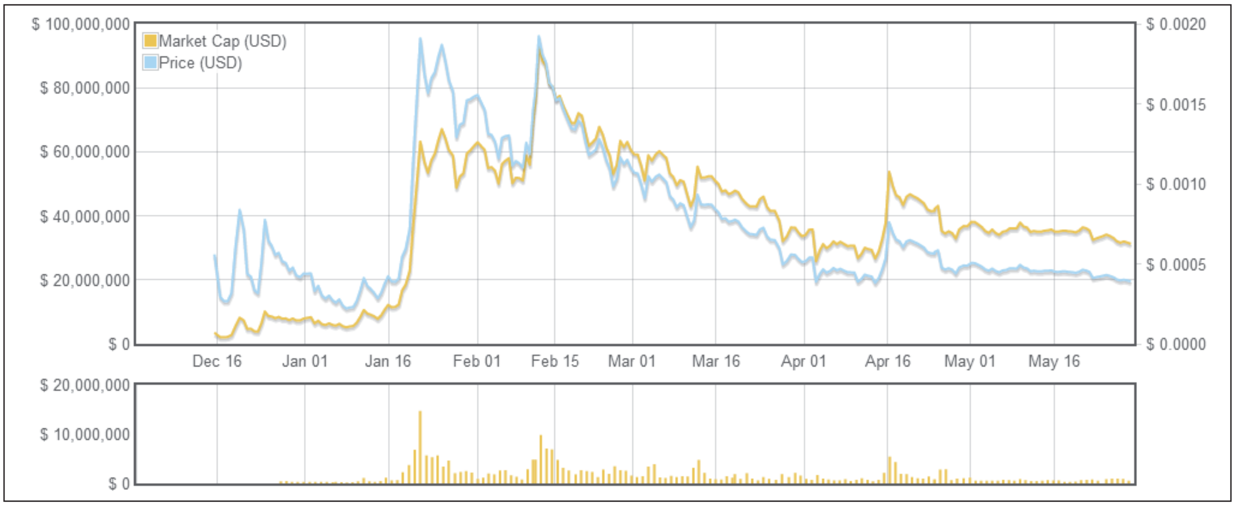


Figure 9: DOGE market capitalization vs. DOGE USD value (last 180 days chart from 30 May 2014) [12].

trying to push the limits (and/or patience) of a well-funded and well-lawyered individual. At the moment the project remains abandoned, although the official logo has been changed to a half-man-half-fish hybrid (wearing sunglasses) in an attempt to demonstrate its disassociation with the hip hop artist's brand.

It wouldn't be painting a complete picture of the current cryptocurrency scene without a mention of an adult-industry-related coin. This industry makes 96 billion dollars every year, with Internet and digital media being at the top of the consumed services. Sexcoin is scrypt based and, with fast transaction confirmations (one minute), targets a niche audience involved in adult goods and services. Even though it clearly states it's not just another alternative currency or a bitcoin competitor, it's gaining momentum as more sites and users begin to see it not as a global currency for value speculation, but for exchange of payments. It's also a deflationary currency with a limit of 250,000,000 coins, rewarding miners with 100 coins for each block mined, although some blocks are worth five or 50 times more as an added bonus.

Virtual currencies hold their value when there's a community backing up the growth of the digital ecosystem. Their value is basically derived from demand, and lack of it means the financial death of the currency as it's considered worthless. While most people trust their banks, or the US Treasury or the US Mint, confidence in the digital currency equivalents seems elusive at the moment, especially with all the security incidents witnessed in such a short space of time.

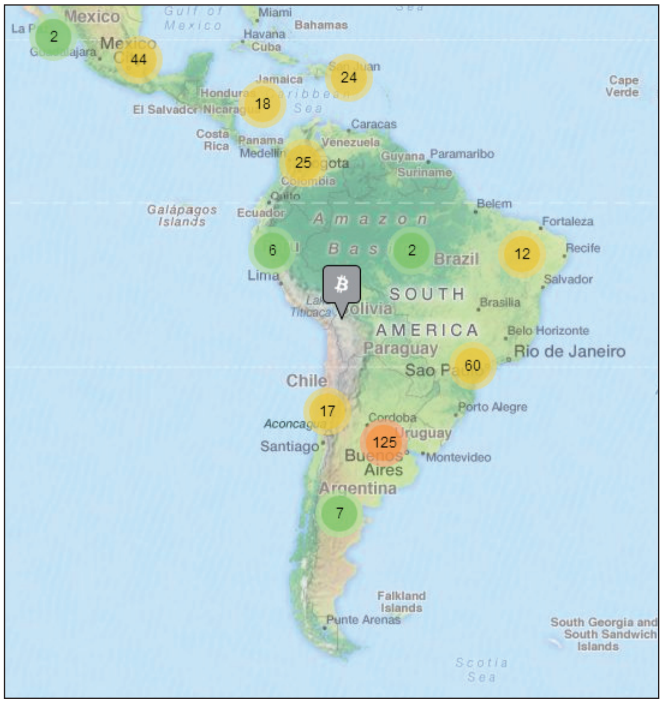
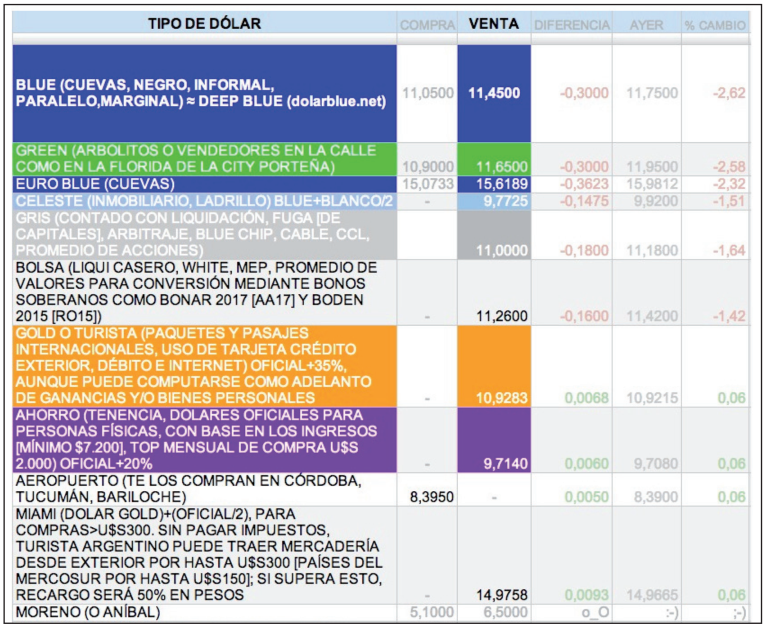


Figure 10: Adoption of bitcoin in Latin America, with Argentina listing 132 merchants accepting payment in this currency.



TIPO DE DÓLAR	COMPRA	VENTA	DIFERENCIA	AYER	% CAMBIO
BLUE (CUEVAS, NEGRO, INFORMAL, PARALELO,MARGINAL) ≈ DEEP BLUE (dolarblue.net)	11,0500	11,4500	-0,3000	11,7500	-2,62
GREEN (ARBOLITOS O VENDEDORES EN LA CALLE COMO EN LA FLORIDA DE LA CITY PORTEÑA)	10,9000	11,6500	-0,3000	11,9500	-2,58
EURO BLUE (CUEVAS)	15,0733	15,6189	-0,3623	15,9812	-2,32
CELESTE (INMOBILIARIO, LADRILLO) BLUE+BLANCO/2	-	9,7725	-0,1475	9,9200	-1,51
GRIS (CONTADO CON LIQUIDACIÓN, FUGA [DE CAPITALES], ARBITRAJE, BLUE CHIP, CABLE, CCL, PROMEDIO DE ACCIONES)		11,0000	-0,1800	11,1800	-1,64
BOLSA (LIQUI CASERO, WHITE, MEP, PROMEDIO DE VALORES PARA CONVERSIÓN MEDIANTE BONOS SOBERANOS COMO BONAR 2017 [AA17] Y BODEN 2015 [RO15])	-	11,2600	-0,1600	11,4200	-1,42
GOLD O TURISTA (PAQUETES Y PASAJES INTERNACIONALES, USO DE TARJETA CRÉDITO EXTERIOR, DÉBITO E INTERNET) OFICIAL+35%, AUNQUE PUEDE COMPUTARSE COMO ADELANTO DE GANANCIAS Y/O BIENES PERSONALES	-	10,9283	0,0068	10,9215	0,06
AHORRO (TENENCIA, DOLARES OFICIALES PARA PERSONAS FÍSICAS, CON BASE EN LOS INGRESOS [MÍNIMO $7.200], TOP MENSUAL DE COMPRA U$S 2.000) OFICIAL+20%	-	9,7140	0,0060	9,7080	0,06
AEROPUERTO (TE LOS COMPRAN EN CÓRDOBA, TUCUMÁN, BARILOCHE)	8,3950	-	0,0050	8,3900	0,06
MIAMI (DOLAR GOLD)+(OFICIAL/2), PARA COMPRAS>U$S300. SIN PAGAR IMPUESTOS, TURISTA ARGENTINO PUEDE TRAER MERCADERÍA DESDE EXTERIOR POR HASTA U$S300 [PAÍSES DEL MERCOSUR POR HASTA U$S150]; SI SUPERA ESTO, RECARGO SERÁ 50% EN PESOS	-	14,9758	0,0093	14,9665	0,06
MORENO (O ANÍBAL)	5,1000	6,5000	o_O	:-)	;-)

Figure 11: Latin American websites list not only (the many) black dollar and euro value rates, but also bitcoin rates.

THE ECONOMY IN LATIN AMERICA – A THRIVING GROUND FOR CRYPTOCURRENCIES

With a dollar black market that has always been part of the Argentinian culture, and the dollar 'blue' value published next to the official one each morning in the papers, cryptocurrencies have found their place in Argentina. On taking a walk down Florida Street in Buenos Aires, you will see the best shops the city has to offer. You'll also hear the yells of 'Cambio!' as the many 'arbolitos' offer you black market rates for your dollars and euros, all in plain sight.

After the financial crisis suffered in 2001, where the famous one peso for one dollar 'Ley de Convertibilidad' was no longer valid, the local currency began a strong devaluation process that still continues to the present day. With many citizens hoping to avoid the monetary erosion of their savings by seeking security in the American currency, those who were trapped in the 'corralito' weren't so lucky and couldn't touch a single dime of their money. The confidence in the government (any of them) and the local currency have been in the spotlight ever since, and rebuilding trust is not an easy process. Several other countries in Latin America have witnessed similar circumstances of strict currency control and inflationary processes in conjunction with the rapid devaluation of the local currency. The working class has resorted to alternative currencies and investment options as a means of preserving value in these uncertain times.

Hiding dollars or euros under a mattress is not unheard of, but what about an encrypted USB drive with your favourite cryptocurrency? According to *CoinMap*, Argentina is leading the pack when it comes to bitcoin adoption, with a great number of small merchants and businesses accepting BTC as a means of payment for goods and services. The adoption rate is significantly higher than that observed in other metropolitan Latin American cities such as Sao Paolo, Mexico City or Santiago de Chile.

Bitpay, a leading bitcoin service provider, has recently opened a regional branch in Argentina, demonstrating the local market potential. In addition, the Argentinian entrepreneur Wenceslao Casares has launched *Xapo*, a second-generation online wallet storage that's amongst the first to offer insurance on the funds stored, and which has received an initial round of investment from several recognized Wall Street firms. *Xapo* is presently working on a debit card linked to your bitcoin wallet that will use the networks of one of the major credit cards, allowing it to work virtually anywhere. But with great power comes great responsibility, and if fraudsters were interested in obtaining your credit and debit card numbers before, the future for them looks even more interesting now.

By holding regular meetings, The Argentinian Bitcoin Foundation explains cryptocurrencies not only to local enthusiasts, but to tax agencies and regulatory entities too. Positioned as a legal way of investing in the local market, it offers Argentinians and people from all over Latin America an investment option that has not been seen before.

Nevertheless, governments are getting frustrated as regulations are not part of bitcoin's design. With Argentina's black market growing, the UIF ('Unidad de Información Financiera') has taken a keen interest in the currency, which challenges current banking institutions and in some cases makes the process of money laundering and the financing of illegal operations easier.

Those escaping tax are familiar with Panama as a financial paradise for setting up their companies. With the arrival of bitcoin, governments are resorting to asking coin holders to kindly pay taxes in order not to make tax evaders' lives any easier. Brazil is setting the trend, with the Brazilian Revenue Service declaring bitcoin taxable in the same way as any other payment would be. With a large percentage of Brazilians acquiring bitcoins via the popular site *Mercado Bitcoin*, authority monitoring seems like a pipe dream at the moment and relies on the honesty of the citizens.

Economy 101 applied to digital currencies

The first mover advantage refers to the advantage gained by the first significant occupant of a market segment. Many alternative coins were pre-mined by their developers in order to conserve some of the financial benefits in case the coins became successful. In this case, if the pre-mined quantity was not significant enough, or the currency was ASICs resistant, mining farms would take over that initial advantage gained. In the bitcoin community, and any cryptocurrency community in general, the phrase 'pre-mined' is an instant turn-off for the many enthusiasts that believe in coins not only as fiat alternatives, but also as an ethical and moral message to governments and regulation authorities. Mining feasibility studies can be performed as a preliminary evaluation that can determine if a resource can be mined economically (profitability). Albeit different from an actual mineral mining study, there are some similarities, but with the volatile nature of currencies a whole economic spectrum opens without even taking into consideration sociological and psychological aspects.

Known as the network effect, the economy concept proposed by Hal Varian states that the value of a product or service depends on the number of others using it. It's one of the reasons why bitcoin remains on the podium while alternative (and subjectively better) cryptocurrencies appear every day. By establishing a firm user base and gaining wide acceptance, the stability of the currency is being guaranteed by its community, who strongly believe in an unspoken social convention that the value of bitcoin in the development of business transactions will remain as a viable option.

As a deflationary currency (no more units will be created after the 21 million limit is reached), bitcoin brings into the spotlight the topic of velocity of money. When there's inflation there's incentive for currency holders to spend it, but if no more units are created then we could face the tragedy of the commons where individuals acting out of their own interest (hoarding) could harm the currency's health, causing the unit's value to plummet.

When someone such as Warren Buffett warns the general public to stay away from bitcoin, claiming a lack of intrinsic value and reducing it to a mere system for moving funds from point A to point B, it creates an equally passionate response from the other side of the table. Marc Andreessen, Internet pioneer, trusts that none of the points mentioned previously will cause the demise of the currency but would only make it stronger and more valuable.

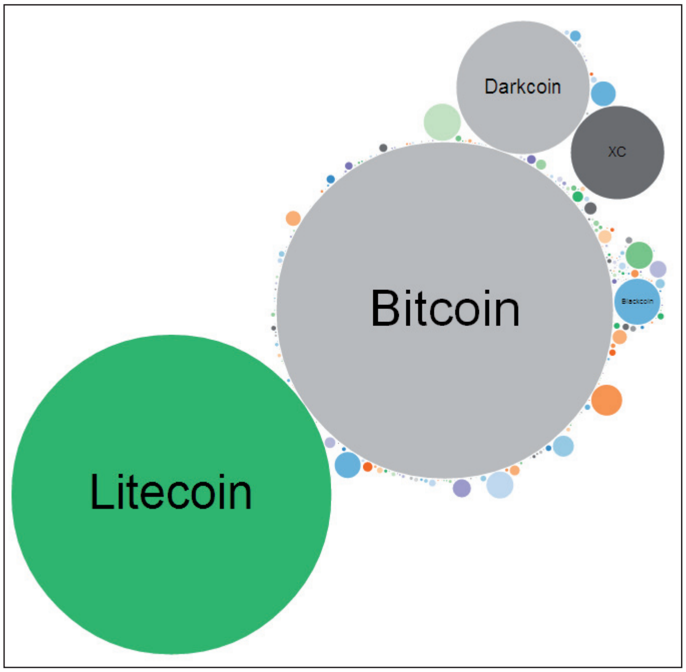


Figure 12: Network effect regarding bitcoin adoption [13].

Intrinsic value theory holds that the value of an object, good or service is contained within the item itself. Bitcoin transcends nations, politics, religions, cultures and regulations, allowing the movement of funds across borders with minimal or no fees at all, and without third-party intervention. In countries suffering from hyperinflation, where citizens need a way out of the system, this becomes quite important, moving freely from banking and government rules, laws and restrictions. These special properties make the subjective value of bitcoin much more relevant than what the naked eye can see.

Giving countries in the midst of economic crisis, such as Zimbabwe, an option of bank-free operation and avoiding costly exchange rates seems like a utopia. Even though African countries have been hesitant about utilizing bitcoin for everyday transactions due to concerns about money laundering, they are beginning to see the benefits and starting to negotiate with mobile payment vendors. On the other hand, we have Mexico, with *Bitso*, a digital currency exchange launching a Ripple gateway for Mexicans to easily transfer remittances in pesos, USD dollars, BTC or XRP (Ripple network unit) across borders. With billions of dollars sent from the US to Mexico each year, the ability to send cash back home is vastly simplified with the use of cryptocurrencies and networks of trust which allow the movement of any currency between participants.

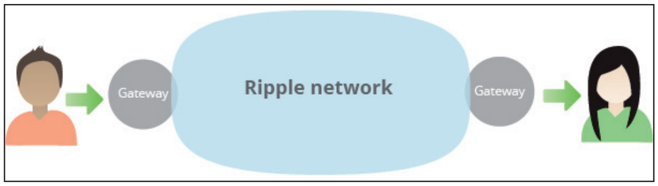


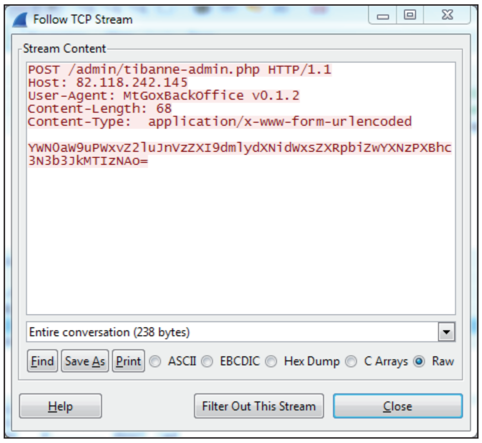
Figure 13: The inner workings of Ripple networks are quite simple and based on the trust held between parties [14].

> *'Our concern is, and the government's concern is, money laundering. So we need to kind of be the poster children of how to do [compliance] correctly. So I'm not going to launch [a fiat currency option] until I'm ready to be on the poster.'* – Paul Vernon, Cryptsy founder.

Then the malware comes

We have seen why Latin America has become a fertile ground for the adoption of a cryptocurrency economy – unfortunately, so too have the cybercriminals. With a whole new set of frauds, scams and threats, citizens need to be aware that keeping their savings secure is not an easy task in today's hyper-connected world. Just as there are no borders for cryptocurrencies, there are none for criminals either, and following the money trail means landing in Latin America, where the general audience is still widely vulnerable to many of the attacks seen in other parts of the world.

After the *Mt. Gox* incident, we have witnessed targeted phishing campaigns, bitcoin community members moonlighting as private investigators, localized ransomware samples, scams, mobile miners, Internet of things devices participating in botnets, and anything in between.



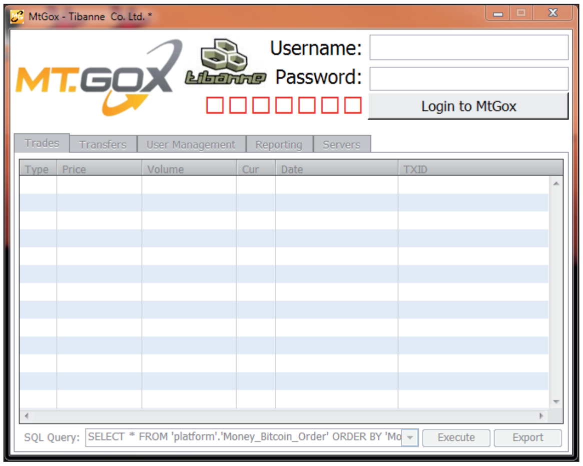
```
POST /admin/tibanne-admin.php HTTP/1.1
Host: 82.118.242.145
User-Agent: MtGoxBackOffice v0.1.2
Content-Length: 68
Content-Type:  application/x-www-form-urlencoded

YWN0aW9uPWxvZ2luJnVzZXI9dmlydXNidWxsZXRpbiZwYXNzPXBhc
3N3b3JkMTIzNAo=
```

Entire conversation (238 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 14: Mt. Gox trojan sending base64-encoded credentials to a remote server in Sofia, Bulgaria.



SQL Query: SELECT * FROM 'platform'.'Money_Bitcoin_Order' ORDER BY 'Mo

Figure 15: Mt. Gox's fake back-end client which tricked victims into supplying their credentials.

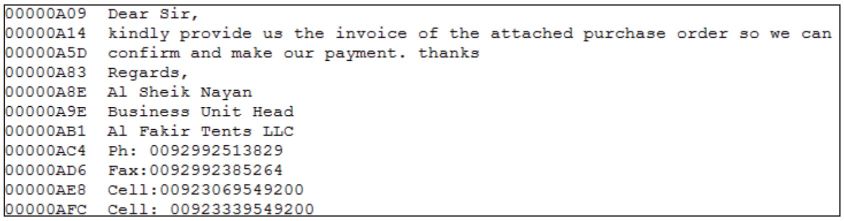
MALWARE IN THE BITCOIN ECOSYSTEM

As mentioned in the *Kaspersky*'s 2013 Security Bulletin, the predictions made for the cybercriminal bitcoin ecosystem have come true, and then some:

> 'Attacks on Bitcoin pools, exchanges and Bitcoin users will become one of the most high-profile topics of the year. Attacks on stock exchanges will be especially popular with the fraudsters as their cost-to-income ratio is very favourable.
>
> 'As for Bitcoin users, in 2014 we expect considerable growth in the number of attacks targeting their wallets. Previously, criminals infected victim computers and went on to use them for mining. However, this method is now far less effective than before while the theft of Bitcoins promises cybercriminals huge profits and complete anonymity.'

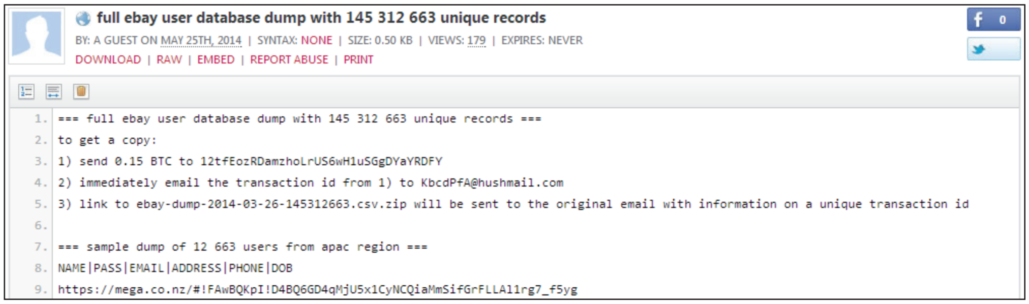
Mt. Gox still alive?

After the rumour that *Mt. Gox* owner Mark Karpeles' blog and *reddit* accounts had been hacked, cybercriminals saw the



```
00000A09  Dear Sir,
00000A14  kindly provide us the invoice of the attached purchase order so we can
00000A5D  confirm and make our payment. thanks
00000A83  Regards,
00000A8E  Al Sheik Nayan
00000A9E  Business Unit Head
00000AB1  Al Fakir Tents LLC
00000AC4  Ph: 0092992513829
00000AD6  Fax:0092992385264
00000AE8  Cell:00923069549200
00000AFC  Cell: 00923339549200
```

Figure 16: Phishing campaign targeting Mt. Gox users (with trojanized compressed executable file).



full ebay user database dump with 145 312 663 unique records

BY: A GUEST ON MAY 25TH, 2014 | SYNTAX: NONE | SIZE: 0.50 KB | VIEWS: 179 | EXPIRES: NEVER

```
=== full ebay user database dump with 145 312 663 unique records ===
to get a copy:
1) send 0.15 BTC to 12tfEozRDamzhoLrUS6wH1uSGgDYaYRDFY
2) immediately email the transaction id from 1) to KbcdPfA@hushmail.com
3) link to ebay-dump-2014-03-26-145312663.csv.zip will be sent to the original email with information on a unique transaction id

=== sample dump of 12 663 users from apac region ===
NAME|PASS|EMAIL|ADDRESS|PHONE|DOB
https://mega.co.nz/#!FAwBQKpI!D4BQ6GD4qMjU5x1CyNCQiaMmSifGrFLLAl1rg7_f5yg
```

Figure 17: After any major breach, a fake credentials dump quickly appears, offering the stolen database for a reasonable sum of bitcoins.

opportunity to design a simple yet effective malicious application, which in conjunction with a publicly believable story, lured several former exchange users into their trap. Using a compressed file named 'MtGox2014Leak.zip', the criminals included several fake spreadsheets with widely available information around *Mt. Gox* finances, and a customized back-end client to access it. Unfortunately, those who thought this was the official interface for *Mt. Gox*'s critical information were infected with a piece of malware designed to steal unencrypted 'wallet.dat' and 'bitcoin.conf' configuration files. At the same time, even though *Mt. Gox* was practically dead, it would contact a remote C&C server, sending the login credentials used in the fake application.

The *Windows* version, detected as Trojan.Win32.CoinStealer.i, and the *Mac OSX* variant, detected as Trojan.Win32.CoinStealer.a, were programmed in the Livecode language in order to easily 'support' several different operating system platforms.

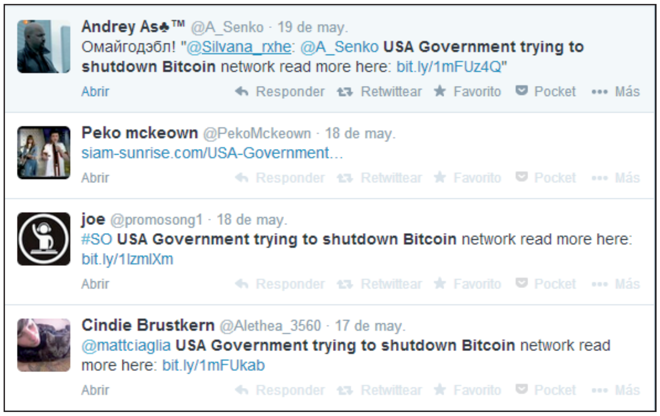
Appealing to the users' curiosity and (in some cases) greed proved effective for the second time. Not too long ago, a mail distributed phishing campaign claiming that former *Mt. Gox* users were required to sign account closure documents was spotted in the wild, also with the clear aim of infecting unsuspecting victims.

Social gold rush and phishing campaigns

Amongst the first bitcoin-related malware samples spotted in Latin America was Trojan.Win32.Jorik.IRC.bot.xkt, which was being spread via *Skype*. At the time, bitcoin mining was still profitable, even with limited CPU resources. Using an initial dropper to download a second-stage payload from the 'HotFile' public file-sharing service gave the victim a copy of the 'cpuminer' mining application, obtaining precious bitcoins for cybercriminals on the other side of the globe.

With the popularity of social networks, bitcoin enthusiast criminals have resorted to spreading their creations via *Facebook*, with a pinch of social engineering as the essential ingredient. As seen previously, very few users can resist the temptation to open a picture, especially when requested to do so by a trusted friend. In reality, these curious individuals would be obtaining a custom developed trojan that searches for unencrypted wallet files. In addition, and even if currently not quite profitable, it would consume computing resources by joining a bitcoin mining pool, expecting to at least get a minimal benefit from the infection.

Numerous phishing campaigns have been spotted before, many of them promising astronomical rates of return for minimal investments, others just promising the user prizes, or announcing the winning of the 'bitcoin lottery'. The same scams and frauds we have seen for many years have added the word



Andrey As♣™ @A_Senko · 19 de may.
Омайгодэбл! "@Silvana_rxhe: @A_Senko **USA Government trying to shutdown Bitcoin** network read more here: bit.ly/1mFUz4Q"

Peko mckeown @PekoMckeown · 18 de may.
siam-sunrise.com/USA-Government...

joe @promosong1 · 18 de may.
#SO **USA Government trying to shutdown Bitcoin** network read more here: bit.ly/1lzmlXm

Cindie Brustkern @Alethea_3560 · 17 de may.
@mattciaglia **USA Government trying to shutdown Bitcoin** network read more here: bit.ly/1mFUkab

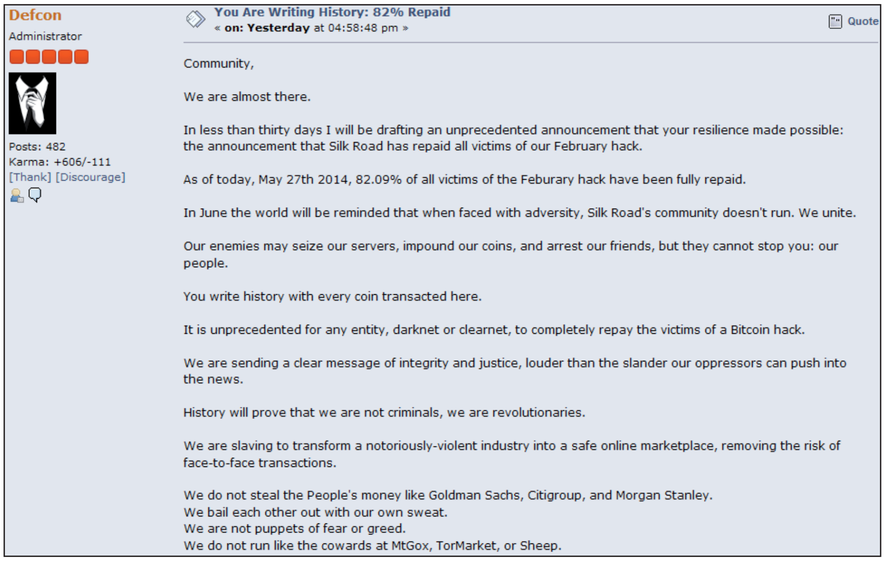
Figure 18: Using the same techniques as seen in other attacks, cybercriminals use the oldest trick in the book: the closure of a service as the hook.

'bitcoin' and are targeting new victims – the game is the same, but the stakes are much higher.

Illegal marketplaces

After the seizure by the FBI of the Silk Road illegal marketplace, new versions started to appear, with the owners putting real effort into regaining the essential trust of their audience. Moreover, the bitcoins lost in this February's hack were promised to be repaid by the site's operators: 'We are committed to getting everyone repaid, even if it takes a year'.

Although not seized but disbanded, Sheep's Marketplace administrators reported that a bug in the system had been responsible for the loss of 5,400 bitcoins. Suspicious of fraud, users in the community donned their private investigator hats with the goal of analysing the public bitcoin blockchain and eventually finding the destination of their (supposedly) stolen goods. A wallet with 96,000 BTC (around 100 million dollars) was the prime suspect of this inquisitive group, composed mainly of angry *reddit* users. But, it was after a taking a closer look that they found the legitimate owner of such millionaire sum, the exchange service *BTC-E*. Currently, *reddit* explicitly prohibits 'doxxing' (publishing personal information) for suspected bitcoin



You Are Writing History: 82% Repaid
« **on: Yesterday** at 04:58:48 pm »

Community,

We are almost there.

In less than thirty days I will be drafting an unprecedented announcement that your resilience made possible: the announcement that Silk Road has repaid all victims of our February hack.

As of today, May 27th 2014, 82.09% of all victims of the Feburary hack have been fully repaid.

In June the world will be reminded that when faced with adversity, Silk Road's community doesn't run. We unite.

Our enemies may seize our servers, impound our coins, and arrest our friends, but they cannot stop you: our people.

You write history with every coin transacted here.

It is unprecedented for any entity, darknet or clearnet, to completely repay the victims of a Bitcoin hack.

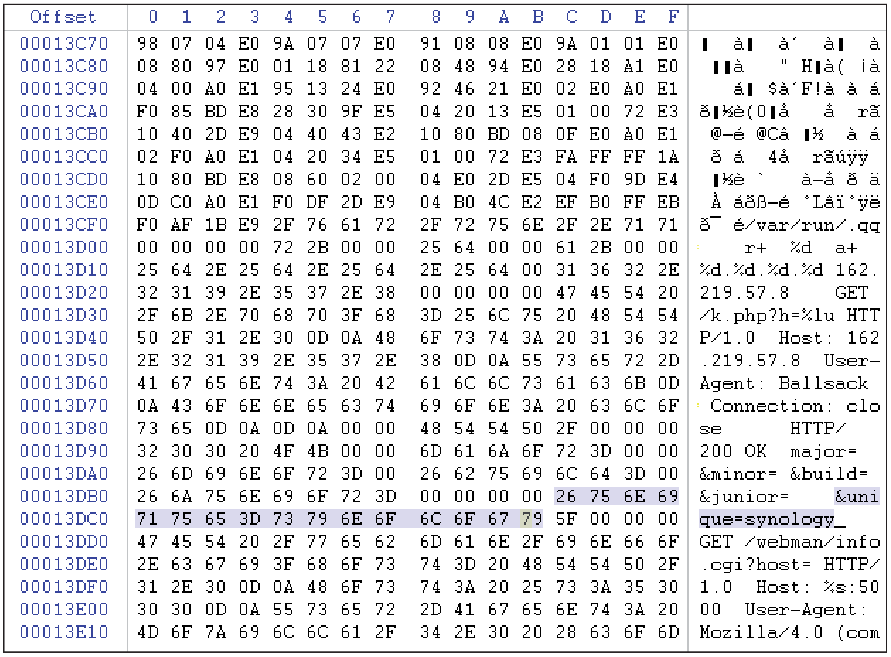
We are sending a clear message of integrity and justice, louder than the slander our oppressors can push into the news.

History will prove that we are not criminals, we are revolutionaries.

We are slaving to transform a notoriously-violent industry into a safe online marketplace, removing the risk of face-to-face transactions.

We do not steal the People's money like Goldman Sachs, Citigroup, and Morgan Stanley.
We bail each other out with our own sweat.
We are not puppets of fear or greed.
We do not run like the cowards at MtGox, TorMarket, or Sheep.

Figure19: Silk Road's administrator, 'Defcon', announcing the repayment of the lost funds to its users.



```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00013C70   98 07 04 E0 9A 07 07 E0  91 08 08 E0 9A 01 01 E0  ▌  à▌  à´  à▌  à
00013C80   08 80 97 E0 01 18 81 22  08 48 94 E0 28 18 A1 E0   ▌▌à   " H▌à( ¡à
00013C90   04 00 A0 E1 95 13 24 E0  92 46 21 E0 02 E0 A0 E1    á▌ $à´F!à à á
00013CA0   F0 85 BD E8 28 30 9F E5  04 20 13 E5 01 00 72 E3  ð▌½è(0▌å   å  rã
00013CB0   10 40 2D E9 04 40 43 E2  10 80 BD 08 0F E0 A0 E1   @-é @Câ ▌½  à á
00013CC0   02 F0 A0 E1 04 20 34 E5  01 00 72 E3 FA FF FF 1A   ð á  4å  rãúÿÿ
00013CD0   10 80 BD E8 08 60 02 00  04 E0 2D E5 04 F0 9D E4   ▌½è `   à-å ð ä
00013CE0   0D C0 A0 E1 F0 DF 2D E9  04 B0 4C E2 EF B0 FF EB   À áðß-é °Lâï°ÿë
00013CF0   F0 AF 1B E9 2F 76 61 72  2F 72 75 6E 2F 2E 71 71  ð¯ é/var/run/.qq
00013D00   00 00 00 00 72 2B 00 00  25 64 00 00 61 2B 00 00      r+  %d  a+
00013D10   25 64 2E 25 64 2E 25 64  2E 25 64 00 31 36 32 2E  %d.%d.%d.%d 162.
00013D20   32 31 39 2E 35 37 2E 38  00 00 00 00 47 45 54 20  219.57.8    GET
00013D30   2F 6B 2E 70 68 70 3F 68  3D 25 6C 75 20 48 54 54  /k.php?h=%lu HTT
00013D40   50 2F 31 2E 30 0D 0A 48  6F 73 74 3A 20 31 36 32  P/1.0  Host: 162
00013D50   2E 32 31 39 2E 35 37 2E  38 0D 0A 55 73 65 72 2D  .219.57.8  User-
00013D60   41 67 65 6E 74 3A 20 42  61 6C 6C 73 61 63 6B 0D  Agent: Ballsack
00013D70   0A 43 6F 6E 6E 65 63 74  69 6F 6E 3A 20 63 6C 6F   Connection: clo
00013D80   73 65 0D 0A 0D 0A 00 00  48 54 54 50 2F 00 00 00  se      HTTP/
00013D90   32 30 30 20 4F 4B 00 00  6D 61 6A 6F 72 3D 00 00  200 OK  major=
00013DA0   26 6D 69 6E 6F 72 3D 00  26 62 75 69 6C 64 3D 00  &minor= &build=
00013DB0   26 6A 75 6E 69 6F 72 3D  00 00 00 00 26 75 6E 69  &junior=    &uni
00013DC0   71 75 65 3D 73 79 6E 6F  6C 6F 67 79 5F 00 00 00  que=synology_
00013DD0   47 45 54 20 2F 77 65 62  6D 61 6E 2F 69 6E 66 6F  GET /webman/info
00013DE0   2E 63 67 69 3F 68 6F 73  74 3D 20 48 54 54 50 2F  .cgi?host= HTTP/
00013DF0   31 2E 30 0D 0A 48 6F 73  74 3A 20 25 73 3A 35 30  1.0  Host: %s:50
00013E00   30 30 0D 0A 55 73 65 72  2D 41 67 65 6E 74 3A 20  00  User-Agent:
00013E10   4D 6F 7A 69 6C 6C 61 2F  34 2E 30 20 28 63 6F 6D  Mozilla/4.0 (com
```

Figure 20: Synology NAS devices used to mine cryptocurrencies using an embedded version of CPU Miner.

thieves since there have been so many false positives leading to never-ending witch hunts.

With bitcoin anonymizing services like ‘Bit Fog’ or ‘Dark Wallet’, using the public ledger as the sole evidence for finding cybercriminals will prove a daunting task in the near future. By taking money from different sources, mixing them in a single wallet and spitting out a different amount at the other end of the transaction, money laundering techniques will be deeply ingrained in the bitcoin community’s technical repertoire.

Ransomware in Latin America

A plethora of locally reported ransomware cases have forced some business owners to learn the meaning of ‘bitcoin’. Demanding a payment to recover encrypted files has left many small and medium-sized companies wondering what went wrong. Of course, cybercriminals understand the financial crisis suffered by many Latin American countries, and offer reduced rates to victims in dire need of recovering their files.

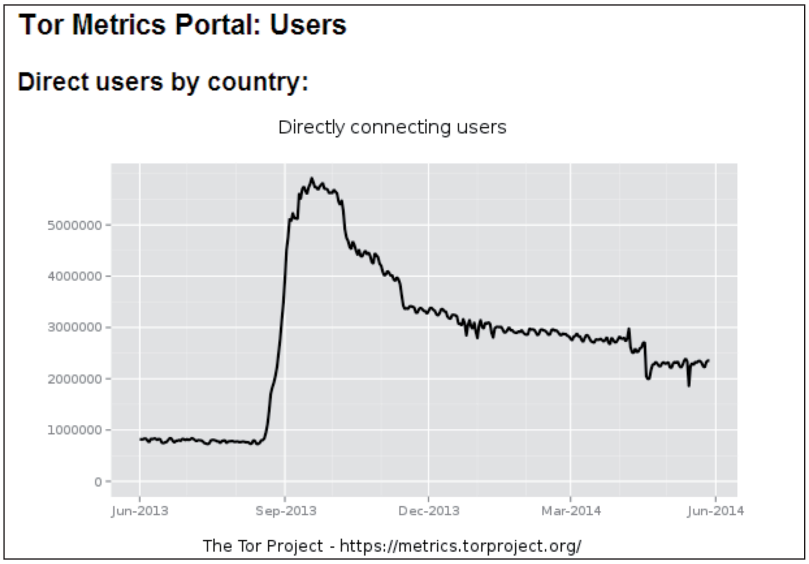


Figure 21: Increase in connecting TOR users between June and September 2013 due to the Sefnit mining botnet [15].

Asking for a demonstration that hostage-held files can indeed be recovered is the first option victims choose when faced with a ransomware situation. After being convinced that a payment is due, negotiations begin, and acquiring the bitcoins demanded is another problem in itself, given the strict financial controls that are in place in the region.

CrytptoLocker was no doubt famous in the ransomware scene, but a new player called BitCrypt has appeared, adding an interesting functionality for stealing funds present in wallets from several different cryptocurrencies. The combination of cryptography, cryptocurrencies, and in many cases *TOR* (to access the payment site), left its victims with a headache and unusable files.

Sometimes providing a TOR2Web URL to facilitate the recovery procedure, cybercriminals appeared to take into consideration the victim’s needs. With ransom values ranging from a couple of hundred dollars to a couple of thousand, users are learning the valuable lesson of having a solid backup policy.

The Reveton ransomware family has upped the ante, also including mining clients with its malicious distributions, making the victims pay a ransom even if unaware of it. The interest that cybercriminals show in bitcoin is not for ethical or moral reasons, but because of the privacy and ease that it provides in managing their illegal operations.

Internet of bitcoin things

Malware that infects digital video recorders has been found, and not even NAS devices, routers and other *Linux*-embedded equipment have escaped this peculiar threat. With very limited resources to spare, malware writers thought it would be useful to put these ‘always-on’ computers to use in mining cryptocurrencies. Of course, even if choosing to mine an alternative coin, the benefits were minimal in comparison to the stress that these devices needed to suffer.

Microsoft destroying the bitcoin-mining botnet Sefnit might look like an unnecessary measure currently, with the increasing difficulty rates of the bitcoin currency. However, with many scrypt-based alternatives still mineable by everyday PCs, cybercriminals will take that opportunity even if there’s little to gain from it. Sefnit’s culprit was the very mechanism designed to protect it: the usage of *TOR*.

Mining from your mobile

The rarest samples of bitcoin-mining malware are not *OSX*-related, even if those are pretty uncommon to find. Using a cracked *Angry Birds* installer in *Mac* (i.e. OSX/CoinThief.A) as a way of infecting bitcoin users seems quite ordinary in comparison to putting a mobile phone to use in mining bitcoins.

As mentioned, embedded devices (DVRs, routers etc.) have little processing power to spare, but at least they have a continuous power source that they can rely on. With smartphones, overheating and excessive battery and bandwidth usage due to malware infections controlling the resources of the device are a giveaway sign.

Two malicious mining applications have been found in the official *Google Play* store, one named ‘Songs’ and the other one ‘Prized’. The threat included in these seemingly innocent applications, known as CoinKrypt, instructed infected phones to mine litecoin, dogecoin and casinocoin. With more than a million downloads for ‘Songs’, averaging a mining rate around 8KH/s per device, the malicious pool just wasn’t enough to make it worthwhile for the developers.

Another trojan, found in fake ‘Tune In Radio’ or ‘Football Manager Handled’ application downloads, focused mainly on mining dogecoin, hence being named by the security community ‘MuchSad’, in reference to the grammatically incorrect cryptocurrency. Again, obtaining marginal profits for their creators, these mobile samples proved (without much surprise) that mining in these devices was not practical or efficient at all.

Then BadLepricon appeared, also in the official *Google* store, this time targeting bitcoin via a hidden mining client, checking the device's battery life and other parameters to stay undetected for as long as possible. One thing all these applications have in common is the usage of social engineering techniques to convince the user of their legitimacy, and to entice them to download them to their devices.

CONCLUSION: BEING YOUR OWN BANK IS MORE DIFFICULT THAN IT SEEMS

Seen by outsiders as a hobby for geeks, bitcoin is more than a currency, it's a community that has certain values ingrained and it's revolutionizing the financial world as we currently know it.

Collective but anonymous, organized yet decentralized, this ordered chaos is beginning to make sense after all the problems it has faced. The closure of many of the exchanges that were once available is bringing a Darwinian equilibrium to the bitcoin ecosystem, forcing those that are left to implement better business practices and security measures.

Malware trends indicate that cybercriminals are migrating from mining botnets and pools to more direct wallet-stealing and exchange credential hijacking methods. As highlighted by the inefficient mining trojans in mobile devices, accessing the funds stored in the victims' digital wallets seems much more straightforward than putting the effort into building a massive network of miners that reap minimal gains.

Debit cards linked to bitcoin wallets are starting to appear and this brings another enticing entry point for criminals. With 'bitwashing' services becoming more common, tracking stolen funds will prove much more difficult in the future, exposing the true anonymous nature of cryptocurrencies.

Once the de facto choice for drug dealers and illegal markets, bitcoin is aiming to gain the global trust of other types of merchants, hoping that the community backing it up will be ready for when it becomes the default standard for online and offline transactions.

REFERENCES

[1] More users, more attacks: Kaspersky Lab stats show a surge in Bitcoin cybercrime. http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-stats-show-a-surge-in-Bitcoin-cybercrime.

[2] Decker, C. Wattenhofer, R, Bitcoin Transaction Malleability and Mt.Gox. http://arxiv.org/abs/1403.6676.

[3] [Bitcoin-development] To prevent arbitrary data storage in TXOUTs — The Ultimate Solution. http://sourceforge.net/p/bitcoin/mailman/message/30705609/.

[4] Bitcoin Weaknesses. https://en.bitcoin.it/wiki/Weaknesses.

[5] Bitcoin Pool Hash Rate Distribution. https://blockchain.info/pools.

[6] Warning: Litecoin Miners Need To Leave Coinotron. http://www.cryptocoinsnews.com/news/warning-litecoin-miners-need-leave-coinotron/2014/05/20.

[7] Litecoin Pool Hash Rate Distribution. https://www.litecoinpool.org/pools.

[8] Bitcoin Exchanges Buckle Under DDoS Attacks. http://www.darkreading.com/attacks-and-breaches/bitcoin-exchanges-buckle-under-ddos-attacks/d/d-id/1113809.

[9] Bitcoin Core version 0.9.1 released. https://bitcoin.org/en/release/v0.9.1.

[10] CVE Details – Bitcoin Security Vulnerabilities. http://www.cvedetails.com/vulnerability-list/vendor_id-12094/Bitcoin.html.

[11] List of Bitcoin Heists. https://bitcointalk.org/index.php?topic=576337.

[12] Crypto-Currency Market Capitalizations. https://coinmarketcap.com/doge_180.html.

[13] Crytpocoincharts – Currency Usage – Graphical Comparison. https://www.cryptocoincharts.info/v2/coins/graphicalComparison.

[14] Ripple – The Future of Payments. https://ripple.com/.

[15] TOR Metrics Portal. https://metrics.torproject.org/.

[16] Mt. Gox: Where are the Bitcoins? http://bitcoinbarbie.com/mt-gox-where-are-the-bitcoins/.

[17] Are crypto-currencies the future of money? http://www.bbc.com/news/business-27200665.

[18] How bitcoin is moving money in Africa. http://www.usatoday.com/story/money/business/2014/04/25/ozy-bitcoin-africa-currency/8148853/.

[19] The World's First Bitcoin Debit Card Is Almost Here. http://www.wired.com/2014/04/xapo/.

[20] You Say Bitcoin Has No Intrinsic Value? Twenty-two Reasons to Think Again. http://bitcoinmagazine.com/12846/you-say-bitcoin-has-no-intrinsic-value-twenty-two-reasons-to-think-again/.

[21] Bitcoin Battle: Warren Buffett vs. Marc Andreessen. http://www.forbes.com/sites/kashmirhill/2014/03/26/warren-buffett-says-bitcoin-is-a-mirage-why-marc-andreessen-thinks-hes-wrong/.

[22] How Fraud Attacks on Bitcoins Are Changing. http://www.banktech.com/risk-management/how-fraud-attacks-on-bitcoins-are-changi/240168089.

[23] Bitcoin's backers know they need to win you over. http://www.pcworld.com/article/2111940/bitcoins-backers-know-they-need-to-win-you-over.html.

[24] A history of bitcoin hacks. http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency.

[25] Recovering stolen bitcoin: a digital wild goose chase. http://www.theguardian.com/technology/2013/dec/09/recovering-stolen-bitcoin-sheep-marketplace-trading-digital-currency-money.

[26] Ripple Network Expands to Mexico With Addition of First Peso Issuer. http://www.coindesk.com/ripple-network-expands-addition-first-peso-issuer/.

[27] La explosión de Bitcoin en Argentina. http://esblog.panampost.com/editor/2014/05/12/la-explosion-de-bitcoin-en-argentina/.

[28] How Bitcoin is Thriving in Argentina’s Black Market Economy. http://www.coindesk.com/bitcoin-thriving-argentinas-black-market-economy/.

[29] Brazil Follows IRS, Declares Bitcoin Gains Taxable. http://www.forbes.com/sites/kenrapoza/2014/04/07/brazil-follows-irs-declares-bitcoin-gains-taxable/.

[30] La oficina antilavado y el Banco Central, con la mira en el bitcoin. http://www.infobae.com/2014/04/20/1558483-la-oficina-antilavado-y-el-banco-central-la-mira-el-bitcoin.

[31] Bitcoin: fiebre argentina por la máquina de dinero digital. http://www.lanacion.com.ar/1596773-bitcoin-pasion-argentina-por-la-nueva-maquina-de-hacer-billetes-digitales.

[32] Argentina is all about the black market Benjamins. http://www.globalpost.com/dispatch/news/regions/americas/argentina/130705/argentine-black-market-usd-dollar-peso-forex.

[33] Inflation in Argentina – New data, old qualms. http://www.economist.com/blogs/americasview/2014/02/inflation-argentina.