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...
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].

![Figure 2: Any content inserted in the blockchain will persist for the lifetime of the bitcoin network.](image-url)

**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.
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.

Figure 6: CVE details datasource query for bitcoin software and protocol-related vulnerabilities, displaying a predominance of DoS vulnerability type [10].
600,000 USD was enough to demonstrate the importance of the ever firing a single gunshot, attackers demonstrated that we had online storage stolen on 2 March 2014, with 896 bitcoins Flexcoin exchanges. all make great learning tools for the new generation of bitcoin engineering approaches, and the rest to bad business practices can attribute the success of some attacks to faulty technical implementations of the bitcoin wallet, others to clever 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 OS X 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
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 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 7: List of bitcoin heists with the most media coverage [11] shown in a logarithmic scale. Values taken from approximate historical BTC prices [12].
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 8:** Market capitalization in USD as of 30 May 2014.

**Figure 9:** DOGE market capitalization vs. DOGE USD value (last 180 days chart from 30 May 2014) [12].
WELL, THAT ESCALATED QUICKLY... PONTIROLI

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.

THE ECONOMY IN LATIN AMERICA – A THRIVING GROUND FOR CRYPTO CURRENCIES

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 Argumentian entrepreneur Wenceslaao 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 Argumentian 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 Argumentians 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 Andreesen, Internet pioneer, trusts that the currency but would only make it stronger and more valuable.
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.

‘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.

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
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

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

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

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

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 ‘doxing’ (publishing personal information) for suspected bitcoin

![Figure 19: Silk Road's administrator, 'Defcon', announcing the repayment of the lost funds to its users.](image19)

<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>0013C70</td>
<td>08</td>
<td>07</td>
<td>04</td>
<td>E0</td>
<td>9A</td>
<td>07</td>
<td>E0</td>
<td>91</td>
<td>0E</td>
<td>08</td>
<td>E0</td>
<td>9A</td>
<td>01</td>
<td>01</td>
<td>E0</td>
<td>91</td>
</tr>
<tr>
<td>0013C80</td>
<td>08</td>
<td>07</td>
<td>07</td>
<td>E0</td>
<td>99</td>
<td>01</td>
<td>18</td>
<td>31</td>
<td>22</td>
<td>09</td>
<td>46</td>
<td>94</td>
<td>E0</td>
<td>9D</td>
<td>28</td>
<td>A1</td>
</tr>
<tr>
<td>0013C90</td>
<td>04</td>
<td>00</td>
<td>0A</td>
<td>9E</td>
<td>13</td>
<td>24</td>
<td>E0</td>
<td>92</td>
<td>46</td>
<td>21</td>
<td>E0</td>
<td>02</td>
<td>E0</td>
<td>9A</td>
<td>E1</td>
<td>01</td>
</tr>
<tr>
<td>0013CA0</td>
<td>00</td>
<td>00</td>
<td>0A</td>
<td>9E</td>
<td>13</td>
<td>24</td>
<td>E0</td>
<td>92</td>
<td>46</td>
<td>21</td>
<td>E0</td>
<td>02</td>
<td>E0</td>
<td>9A</td>
<td>E1</td>
<td>01</td>
</tr>
<tr>
<td>0013CB0</td>
<td>00</td>
<td>00</td>
<td>0A</td>
<td>9E</td>
<td>13</td>
<td>24</td>
<td>E0</td>
<td>92</td>
<td>46</td>
<td>21</td>
<td>E0</td>
<td>02</td>
<td>E0</td>
<td>9A</td>
<td>E1</td>
<td>01</td>
</tr>
<tr>
<td>0013CC0</td>
<td>00</td>
<td>00</td>
<td>0A</td>
<td>9E</td>
<td>13</td>
<td>24</td>
<td>E0</td>
<td>92</td>
<td>46</td>
<td>21</td>
<td>E0</td>
<td>02</td>
<td>E0</td>
<td>9A</td>
<td>E1</td>
<td>01</td>
</tr>
<tr>
<td>0013CD0</td>
<td>00</td>
<td>00</td>
<td>0A</td>
<td>9E</td>
<td>13</td>
<td>24</td>
<td>E0</td>
<td>92</td>
<td>46</td>
<td>21</td>
<td>E0</td>
<td>02</td>
<td>E0</td>
<td>9A</td>
<td>E1</td>
<td>01</td>
</tr>
<tr>
<td>0013CE0</td>
<td>00</td>
<td>00</td>
<td>0A</td>
<td>9E</td>
<td>13</td>
<td>24</td>
<td>E0</td>
<td>92</td>
<td>46</td>
<td>21</td>
<td>E0</td>
<td>02</td>
<td>E0</td>
<td>9A</td>
<td>E1</td>
<td>01</td>
</tr>
<tr>
<td>0013CF0</td>
<td>00</td>
<td>00</td>
<td>0A</td>
<td>9E</td>
<td>13</td>
<td>24</td>
<td>E0</td>
<td>92</td>
<td>46</td>
<td>21</td>
<td>E0</td>
<td>02</td>
<td>E0</td>
<td>9A</td>
<td>E1</td>
<td>01</td>
</tr>
</tbody>
</table>

![Figure 20: Synology NAS devices used to mine cryptocurrencies using an embedded version of CPU Miner.](image20)
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.

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.

Cryptolocker 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


