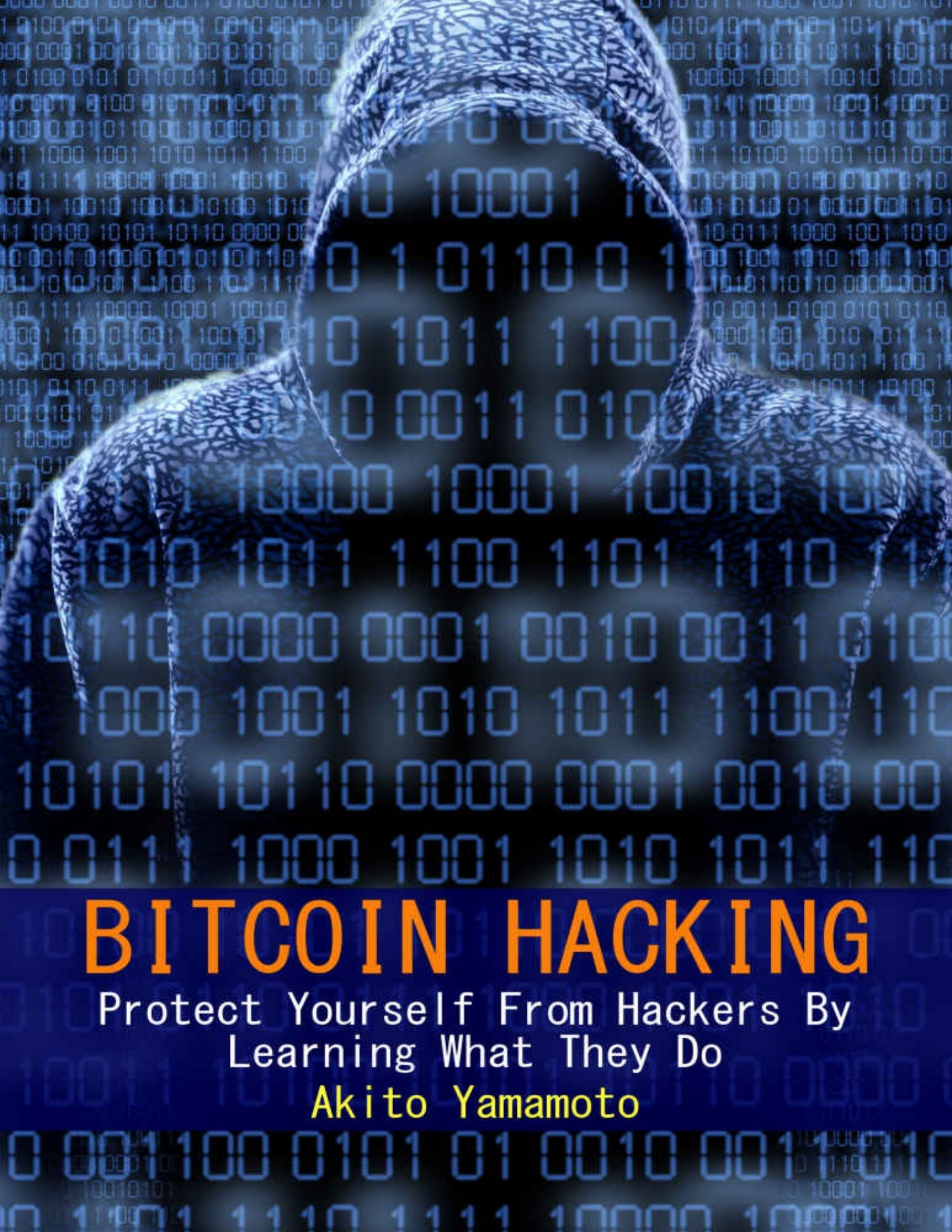


BITCOIN HACKING

Protect Yourself From Hackers By Learning What They Do

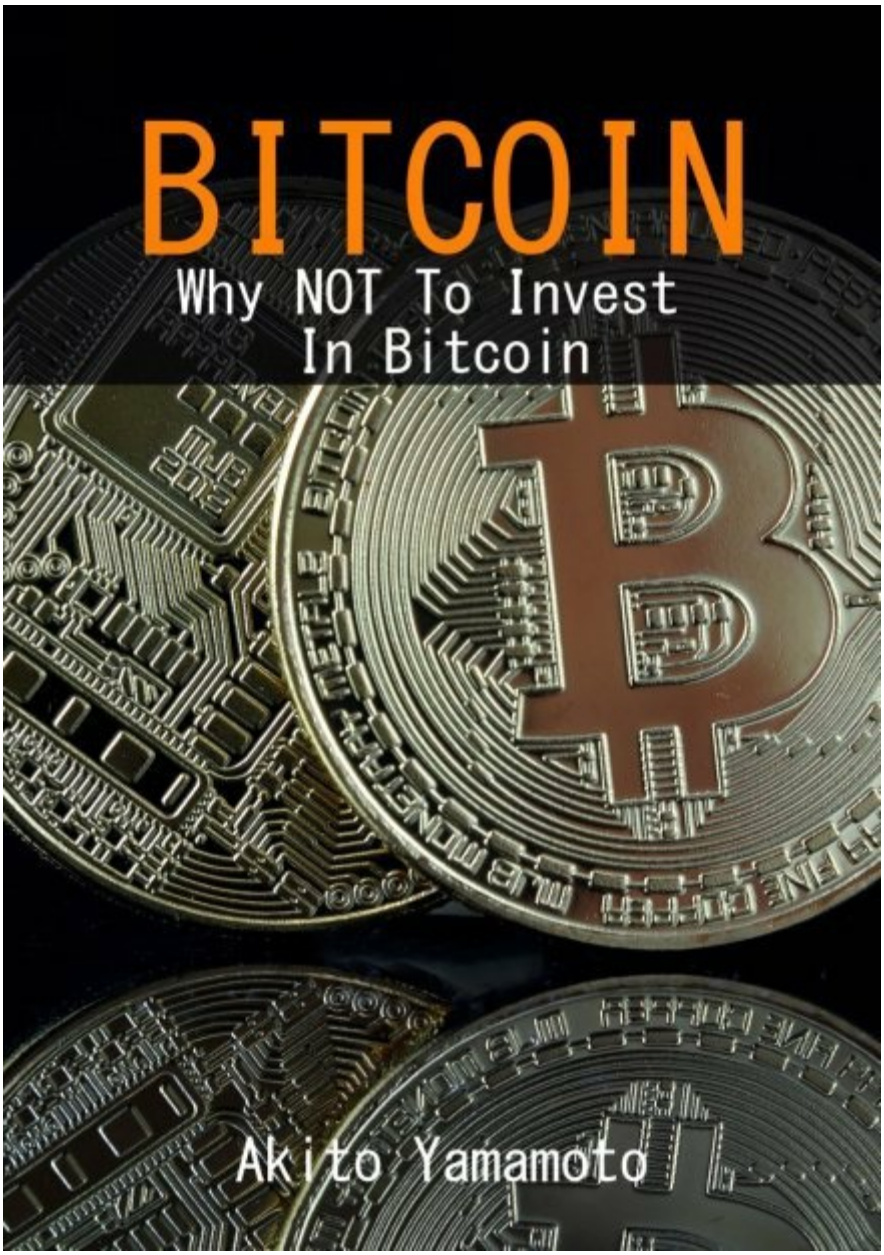
Akito Yamamoto

Bitcoin Hacking

Protect Yourself From Hackers By Learning What They Do

Akito Yamamoto

Click the image of this book, and be directed to the page on Amazon.


BITCOIN
Why NOT To Invest
In Bitcoin
Akito Yamamoto

Intro

Hello to all my readers. I hope you all are investing safely, & wisely? Today let me tell you one short and interesting story that will most definitely be of value to you.

I am sure that you all must have seen movies, many times in your life? In earlier cinema, there was one trending concept that some kidnappers kidnap children of rich people, or sometimes even of their enemies, and then ask for ransom from the victim. Nowadays, after entering into the time of data, this kidnapping has taken new form.

Today data is being kidnapped!

What do kidnappers of today do? They simply get access to your device and encrypt your data, then ask for some ransom, to give you access to your data. Because now data has become most precious to us.

Importance of data can be understood from the fact that we sign up into Ponzi schemes just to get some free data. People sign into their private accounts using public Wi-Fi just because it’s free. These crimes are becoming more and more intense reaching to the limit where now hackers send links to victims to buy bitcoins and send them as ransom. Even bitcoin wallets are also not safe. Neither are the servers from where people buy crypto coins, and not even network on which bitcoin trading is done.

Today I will tell everything I know about bitcoin hacking.

Today we see that investors all over the world are willing to buy bitcoins. Many regular people are doing it also. All this has fueled many startups related with blockchain and crypto currencies.

Even many new crypto currencies are being launched in the market; a wave of unpredicted startups is seen. Nonetheless, many investors still don't know about security related issues.

Bitcoin was launched in 2009 as something which can eliminate third party in trade. It was in the decentralized form. Which means that no one will be overlooking over it. There won't be any administrators who would look after the related issues to solve upcoming disputes. In case of fiat money, the government overlooks and is answerable to all issues and related disputes.

The peer to peer ability of crypto currency have fuelled it's usage. And out of that bitcoin was marketed the most. This helped bitcoin to get a complete hold in the crypto market. It uses a public ledger to record all transactions done.

These bring all of your details into the public and attract hackers.

Many bitcoin wallets are hacked regularly. Even we have heard about attacks on so many cryptocurrency exchanges like in Korea, Mt. Gox. And recently

many happened in Japan. A few crypto mining places are also being hacked like NiceHash. So we can see that even professionals get robbed. Even our investments will also not be safe. Since there is no centralized governing body for bitcoins, it is getting hacked easily and these incidences have increased too much. *Let us get into some case studies to know more about vulnerabilities related to investments in bitcoin, and bitcoin hacking.*

Hacking Case Studies

Attackers took $500,000 in bitcoins from bitcoin user: It was during the time just at the beginning of Bitcoins, when traders just started to accept bitcoins for their services. During this time bitcoin was not famous that much. And had not achieved what it has now. Even at that time, it was able to create a condition of honey attracting bees.

In early 2011. bitcoin was mostly known among geeks. Not even famous ones. Just known among a few of them. We can say it was just a closed community that was including only geeks and hobbyists among them. At this time crypto mining was much easier because of less competition. No one is going to invite a headache (solving difficult puzzles and mathematical functions) for a few pennies. We can conclude that Crypto Mining was so much easier, that it was even possible from a PC. People just sit back for some time solving a puzzle and get thousands of crypto coins. Same was a case of a guy, (we are keeping his name anonymous) who was a permanent user on a bitcoin forum and also a usual crypto miner.

With great fortune and skill he managed to mine 25,000 bitcoins since the start of bitcoin. Now let me tell you guys that though the price of bitcoins was in the pennies at the starting phase. But at the beginning of 2011, it's value reached to $20. So, this guy mined bitcoins worth of $500,000. But then on 13- June- 2011 with some anonymous attack he lost all of his bitcoins.

Those crypto coins were stored in a hard drive. It is believed that some hacker hacked his PC and transferred all 25,000 BTC into some anonymous account. Now, what can be done? Nothing, as there is no responsible figure or authority who can look over disputes related to crypto currencies.

If those bitcoins were not being hacked then it would have been a wealth of $250 million at today's scenario. And all this happened just because hackers overtook his PC and broke into the hard drive. So this was not even a software related issue where reverse tracking is easier. Now again we see that even from the beginning of BTC it was not safe and its ability of not getting traced helps hackers a lot.

A very famous wallet service disappeared: A bitcoin wallet is being bought by a BTC users. When they mine crypto coins they need a wallet to store and get those coins. Bitcoin wallets are such wallets which helped to store bitcoins. One such wallet service provider was MyBitcoins. This bitcoin wallet provider service was very famous in early days of BTC, but all of sudden in month of August in 2011, the service disappeared from the web. Officially the service provider of the mentioned told, that website was hacked and hackers made it disappear from the web.

Many such attacks took place and even bitcoin wallets became vulnerable to hackers.
Now we can see that there is no reliability on BTC, and not even on Bitcoin

wallets.
It’s like buying or renting a locker in a bank where you know vulnerabilities are there. No one will do that. Same is the case here. The place where people store there crypto coins is also not safe. There is no authority to look after them or to call them reliable or to take responsibility of the loss. Even the case may happen where bitcoin wallet service providers, they themselves are frauds, and when they get good amount of BTC, they would just vanish saying some attackers hacked there website. The saying is so easy and narrative can’t be even investigated. So easily all the hard worked earning of BTC by solving puzzles, spending hours in functions, will become just a zero.

So interests and investments in BTC can lead to a total time waste, and 100% of monetary loss since there is no suitable way to verify bitcoin wallets, and we cannot even verify if they say they are attacked by hackers, or it is a well planned out fraud.

Hack into a shared network: This incident took place on March 2012. Here was the case when some attackers took advantage of vulnerabilities present in the shared online web host named then as Linode. Hackers took 46,703 bitcoins from several users of Linode users. In this attack since I told earlier a shared web, Bitcoinica - a very early bitcoin exchange also lost 43,000 bitcoins. All this became possible because of the shared network. As we can see, even today we leave many loops resulting in voids in a network, making it easier to hack into a shared network.

Till now, also we can see that most of the times hacking becomes possible in

public network like wifi or in sharing network. Well soon after in May of same year 2012 that is within 2 months, once again hackers attacked the same network and took away 18,000 BTC from Bitcoinica. To look after all these attacks Bitcoinica went offline for some time and rechecked all security related issues. Even an audit was done within but till now it was too late. As soon after in august 2012 many users of Bitcoinica became angry and sued the company. These users asked for their return which was calculated as high as of $460,000 in deposits. Bitcoincia was unable to survive all this and soon after it declined due to such high loses. All this happened just because of security ignorance in web and sharing networks. This void created while sharing networks can be a minor or major nevertheless it will be always big enough for the attackers to perform their loot into your bitcoin account.

Now, the question comes, what can we learn from this?

As we can see from the Linode case, that this bitcoin business is to be done with extreme security conditions, and operators should always remain extremely careful while accessing BTC related data on sharing network. As most of the bitcoin related data remains in encrypted form, so if someone from inside users get to know about encrypted data, then they can be rouge and transfer all BTC into some online bitcoin account. Then once transferred as we all know it won't be traced so attackers can never be caught.

Shutdown of a very famous BTC saving trust: This was not a digital hacking. Infact I would rather say it as social hacking. Tendon shavers started a trust with the idea of taking BTC with clients and using them as investment, then returning some shares back to its customers. As we can say it is not like that we are going to earn profit each time. Sometimes it will be a loss also,

but operators did not speak a word about that. Such schemes are always a Ponzi, and one should always be able and smart enough to identify them.

Now what this guy did, he took BTC from clients as a form of investments and promised all of them to give weekly return with 7% interest rate on their investments. At the start he attracted many naïve investors and was able to collect nearly about 700,000 BTC or even more from them. To provide returns to investors he used to pay them from the BTC he obtained each time with new investors. Soon this Ponzi scheme was checked by local government and the culprit was caught in August of 2012.

After investigation officials found that the culprit performed more than 700,000 BTC transactions, and all this cost 265,678 BTC to investors, finally shutting down the scheme in august 2012. Then later in 2014 court judge told the culprit to pay back $40 million to all of victim investors.

Hacking of BTC exchange: A bitcoin exchange center helps in converting BTC into fiat currencies or fiat currencies into BTC. A very famous exchange center namely Bitfloor of the time 2012, was attacked by hackers. In this attack network of exchange was hacked and near about a total of 24,000 BTC was transferred into some unknown bitcoin account. Being a bitcoin account, it was difficult to trace transactions, and just the same as it was happening earlier, no one was caught in the act. This cyber theft at that time amounted to about $250,000. Exchange forum Bitfloor did not have reserves of about $250,000, so because of this cyber theft it stopped it’s working for some

time. Well but in this case, exchange center Bitfloor tried their best to return deposits of their customers, and so it started once again just after few weeks of shutdown. But again this effort was unsuccessful and finally the exchange center declared its official shutdown in April of 2013, and its investors were unable to retrieve even their deposit amount from Bitfloor.

A very famous incident of Mt. Gox: Mt. Gox at that time was among the world's biggest bitcoin exchange center during 2014. Mt. Gox was one of the largest financial hubs of bitcoin trading, and it was the only reason why people at that time started buying and selling bitcoins. It was because of the Mt.Gox that bitcoins became so famous from the time of its launch in 2010. The huge foundation was laid by French born CEO Mark Karpeles.

He started operating the firm from the headquarters which were situated in Japan. And since being so famous it will obviously attract hackers. And the same happened as expected. One day in February 2014 it was noticed within the firm that 850,000 bitcoins had gone missing. It was finally announced by the officials of the exchange center stating that they suspected that some hackers are likely to have stolen these bitcoins.

Again as it was happening again. Where there was first a hack reported into privacy, may it be network hard drive or any platform. Then a transfer of BTC into some other anonymous account which cannot be traced because of the ability of BTC remaining anonymous.

Since there is no one responsible for the transaction, so it can't be investigated. These attacks even cause great economical loses, even to countries. This online theft caused $450 million at that time back in February 2014, and now it's worth will be around $9 million. Luckily in this case of massive theft one suspect was arrested by US law enforcement officials in July. He was a Russian man named Alexander Vinnik, this guy had his own bitcoin exchange, where he worked as owner and operator. His firms' name was BTC-e and it was competing firm of Mt.Gox. It was investigated and it came to be known that the suspect knowingly accepted all the stolen bitcoins from hackers into his trade center. He then laundered those BTC through his own exchange center BTC- e, and then was caught by police.

But all this was too late as investors were already angry with exchange center Mt. Gox, which led to the final collapse of Mt. Gox BTC exchange center. But soon after its bankruptcy, BTC value increased once again to new heights. But authorities ordered to freeze all the claimed assets and liabilities of Mt. Gox. And that too in terms of Japanese currency Yen, and at the same time the company was trying to come out of the process of bankruptcy. And soon all the remaining sealed BTC of the exchange center amounting $400 at the time of legal action, achieved very high rates. But since it was not allowed to trade with them, so the company was not even to utilize the last chance it got. And it went to bankruptcy officially. After all this when BTC reached a mark of $11000 then it's former creditors showed the will to get repaid in the same amount, but it was not possible in Japanese law.

Again, in the next year there was one more attack on a very then popular

bitcoin exchange named Bitstamp. At the time during 2015 this Bitstamp was a very famous exchange center, and had great following. This worked as honey for bees around, and attackers were attracted towards it. Soon an attack by hackers took place in it, and the exchange center reported that it lost around 19,000 bitcoins one fine day. These stolen bitcoins were evaluated to cost around then $5 million, making it such a huge amount. But it is only one till now which was able to survive attack and is managing till now with the bitcoin trades. And finally it remained to be one of the leading bitcoin exchanges to date. But we can see even hackers are able to get through securities of such big firms.

And an individual's cyber security is much endangered as compared to big firms. So it is easier for hackers to get into our network system, and hack it as compared to some professional firms. And once bitcoins are transferred, then no one can help.

Again another exchange center was attacked: Again it was a very famous exchange center of its time named Bitfinex. So we see usually, exchange centers seem to be the first choice of hackers. Might be because they are able to get large stock piles of bitcoins at one place, and with one go these hackers manage to get very huge amount of money. Bitcoins are easily laundered in the market again since no identification is present. And even once transferred cannot be traced. In august of 2016 this very famous bitcoin center announced that it had lost 120,000 bitcoins because of cyber theft by some anonymous hackers group. The total worth of the stolen bitcoins was evaluated by the exchange center.

The said declared value was $77 million worth when converted into fiat currency from the stolen amount of bitcoins. However, in this case the exchange center forced this loss on its customers of the time. And to recover its own loss, they planned to pay their customers a redacted value of bitcoins, present value at the time. They forced a reduction of thirty six percent in the deposits of their customers. And let me make you guys aware that this exchange center is still functioning around the globe.

But we need to be careful as it does not have any credibility of its own. Even one of the famous newspapers, New York Times has made a statement related to exchange center Bitfinex. That its operations are not transparent, since the said the exchange center doesn't provide any information related to transactions that are being handled by them. Till now also there is no information that from where this exchange center operates. No country information on its official website. So we all need to remain aware and careful while investing in bitcoins, so that our investment remains secure and can't be hacked by attackers breaking through our hard drive system or even in network.

One of the famous experts Dr. Marco Tomamichel in the field of bitcoins said that most of the existing bitcoin accounts, and all of the new transactions would be at risk within 10 years from now on.

So we need to stay alert, aware, and careful.

I will try to bring up some theories of hacking into the core of bitcoin technology. First theory suggests that if the majority of ledger being updated comes under the influence of hackers. Then they will have enough power to create a parallel network of bitcoins, where all the existing bitcoins will be used, but with different owners. It means then eventually all existing users can lose their bitcoins.

One of the theories suggests that if some group of hackers are able to obtain access of more than the majority of the mining networks, then they can obtain an access to bitcoins blockchain technology. And also they will be able to update and validate ledger according to themselves.

Since ledger contains all the transactions related information's, it will be a dangerous move. Such a group of hackers can block any transactions or even can allow multiple times the use of a single bitcoin.

Many mining centers are increasing rapidly, so maybe in the future this attack theory can be possible. At the present era even there is a possibility of the said theory, as 70% of hash power is within the top 5 largest mining centers. So if they join, it will be above fifty percent, making it a huge majority which would be able to decide what can be done with bitcoins.

Even it can also be organized to make several splits in bitcoins, and then transfer them at different servers. This may result in a new format of peer to

peer transactions. It can be concluded that all these theories if they became practical. Then users will have a shift in new blockchain, which will be driven by a monopoly in the market of related field.

How hacking becomes possible?

Someone gets access to storage accounts by just using your own password: Now since storing crypto coins as we all know, till now, we need an e-wallet. Many service providers provide such services on their online platform. Users of such services need to create a private password, and a public key is created for them.

Now if in this case hackers try to send emails related to the topic, to the users to get their passwords. Once on clicking these links a bug gets activated in the system of users and it releases all information from the users system to the hackers system. In this way, called phishing, people easily lose their data to others. It is simple, but the most common method used by hackers. Sometimes the coincidence meets the level when like if some user has requested to change a password from the service provider, and some hacker creates a phishing page, and sends it to the email of a user using the tag name of service provider. Detailing the email to change the password from the user.

Now since the user has requested to change the password, so with obvious reasons they will be going to fall for the trap, and once the link on the email is clicked, all default information will be send to the hackers.

Brilliant right? Evil, but brilliant!

This mostly happens when an email account does not have two factor safety check, or authentication as we mostly refer to it as. In thr case of bitcoins, since there is no responsibilities decided by any regulating legalized body. It does not have any official security checkup, and every individual needs to handle their security by their own selves. And hence it becomes easy for hackers.

Private key: Well, private key can be seen from bitcoins transaction network, in ledger also. So a hacker can easily get your key, and if they succeed in prompting it, then one will lose its access from bitcoins network, and all its value will become zero. It's better to keep private key in a safe place, in handwritten form, and not make it public to those who are not on any bitcoin network.

Wallet address: A wide range of fake wallet addresses are produced by hackers. This helps them to act like an imposter of bitcoin recipients. Cases are being found when some exchange centers working between some investors and companies, was attacked by hackers. Where hackers formed fake wallets looking completely genuine. These hackers contacted investors and company officials separately. They asked investors to submit money pretending as the related company, and approached companies asking to give bitcoin as investors. Then hackers showed an online fake transaction for both the parties to the exchange centers, making it all to look like genuine process. But soon after getting payment from investors and bitcoins from related

companies, these hackers just disappeared with one go. And it is impossible to trace them.

Insecure third party emails*:* Phishing, one of the most simple and widely used method by hackers in which they produce fake links which are very similar to the original, and look genuine. Sometimes they are so close that there is a difference of only one word in the whole website. So you can understand now how difficult it is to identify fake sites created by hackers. These links are sent to emails. Most of the times these consist of catchy titles like might be offering some free stuff, or asking you to invest in some cheesy schemes.

Once clicked on the link, they take to an unsecure network and a mock up website which looks exactly like original site of the service provider as I have explained above. Then further they might ask the user to enter details. Once one enters details, hackers get access to your privacies in different sites, and they are easily able to transfer bitcoins into their accounts leaving no traces behind.

One such case happened with NiceHash, where hackers were able to get into an employee's system from where they took out the important information related to the bitcoin wallets of the company. Then from the obtained information, they selected one of the famous bitcoin wallets of the company's client, from whose account the hacker took bitcoins costing $64 million.

Dark web users: sometimes hackers are from those among the dark web

users. They create some fake platform related to bitcoins, and start trading. Or any scheme just to bring few investors. And then after collecting enough BTC they suddenly disappear from the web.

Wallets: there are 2 kinds of e- wallets. One is hot wallet other is called cold wallet. These wallets too have few characteristic vulnerabilities making it exposed to hackers, and prone to hacking. Hot wallets are being connected to the internet, and cold wallets opposite to hot wallets, are stored in small storage devices, maybe a usb.

Hacking a payment gateway:

A very unique hacking method is being seen now. Hackers are even able to get into payment gateways. Now in this case hackers don't use any fake phishing link. In fact the link is original, but somehow hackers managed to make the service provider believe that they are original payment gateway. And at same time convincing the clients also the same thing. Further fooling them to transfer bitcoins into their anonymous account, and once it is transferred then nothing can be happened. Same happened with one of the very famous e wallet of Ethereum which is also a crypto currency. In July of 2017 one of the most famous web wallet of Ethereum, Classic cryptocurrency suddenly started stealing money from its users accounts. Later it was found that hackers convinced merchant that they were the real domain holder. And once they got access they took out nearly $300,000 in a few hours only.

Spoofing of payment information:

Sometimes hackers make spoofs of a link and share the link with you. For example if we check some websites and copy it on a clipboard so that we can use it further. What hackers do here is, they use malwares which will change the jumbled address, and will open some page which is not secure.

And if further, you use the same link to do any transactions, then all of it will belong to the hacker, and you yourself will transfer your money to hackers. And usually no one rechecks the address of a copied link on the clipboard, because we think we have just copied it, so how can it be wrong? But actually malware activates when you press or give command of paste, and the address is changed in jumbled form.

Use of key logger softwares:

Many times hackers use key loggers to get the password, and any of the related private initials of users. It stores and sends traces of whatever keys one press on their keyboard.

Hacking of end address:

Sometimes if hackers get access to one's system. With use of malwares, they can easily edit the address of the recipient from the senders device. So that when the sender transfers money, it would be obtained into the hackers account. And since by the time, now we have known that what happens in blockchain remains in blockchain. Imagine transferring 80 BTC to some account, and all the information entered are being double checked, and are correct to the best of knowledge. But as soon as you click to proceed

transaction, you see some different address! But it will be too late to get back your money. This is what happens with the effect of malwares used by hackers.

Hack of important crypto files:

Crypto currency comes with few of the very important files, like wallet files, key files, transaction details files etc. Now usually these files are saved in pc of user. These files can easily be taken or changed by using malwares by hackers.

Once a hacker can successfully to implant a bug, then that's it. Malware will keep doing its job from time to time, sending all important files to the hackers. And in the meantime a hacker can steal all the bitcoins from a users account or e- wallet. Even if these files are stored in hard drive.

Data in encrypted form:

Bitcoin wallets services and other services try to keep their investors related data secure by keeping it in encrypted form. But it can also be a problem, because once a hacker is somehow able to break into it, then at one place everything will be obtained by the attacker, like mining related details, wallets details, website details etc. also bitcoins are secured by encrypted key. So if any rouge employee, or any third party is able to get access to it, which we have seen is very easy by phishing. Then all bitcoins from a firm would

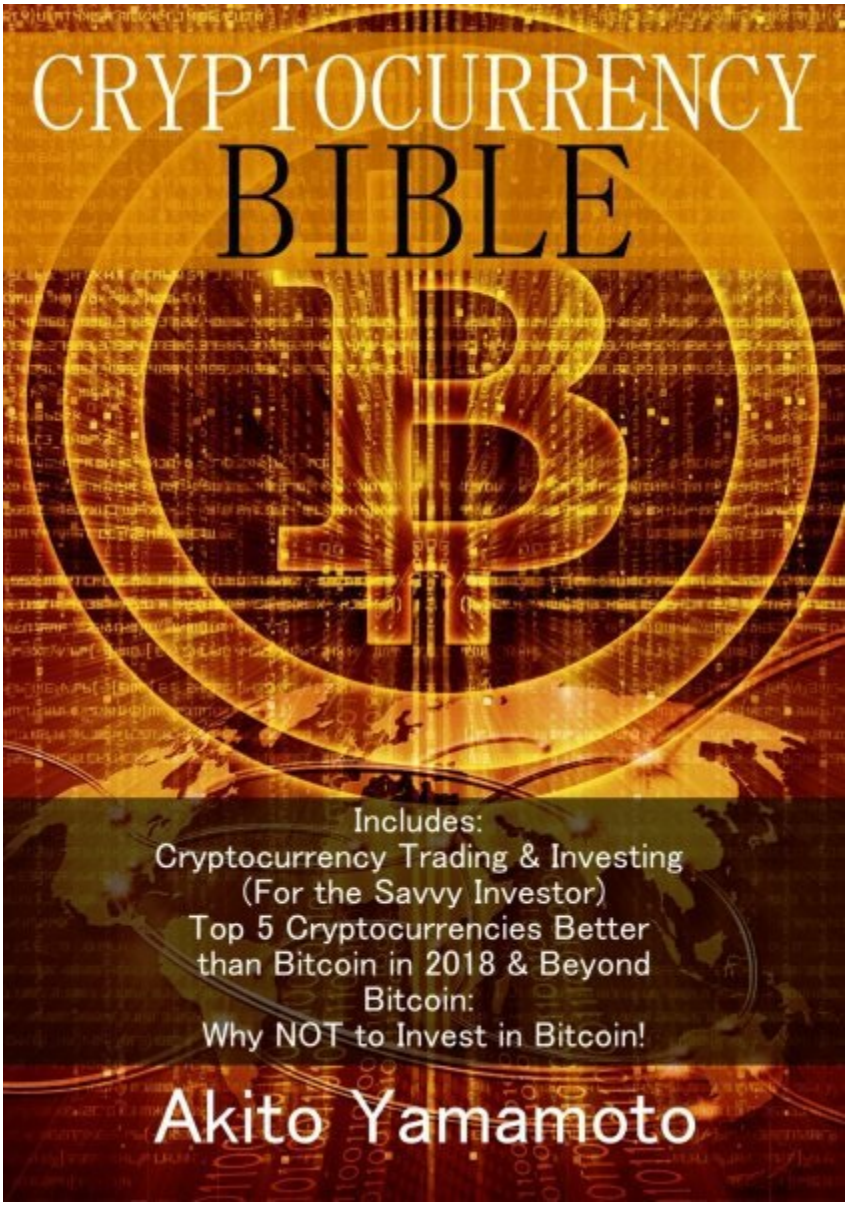
empty down within few minutes.

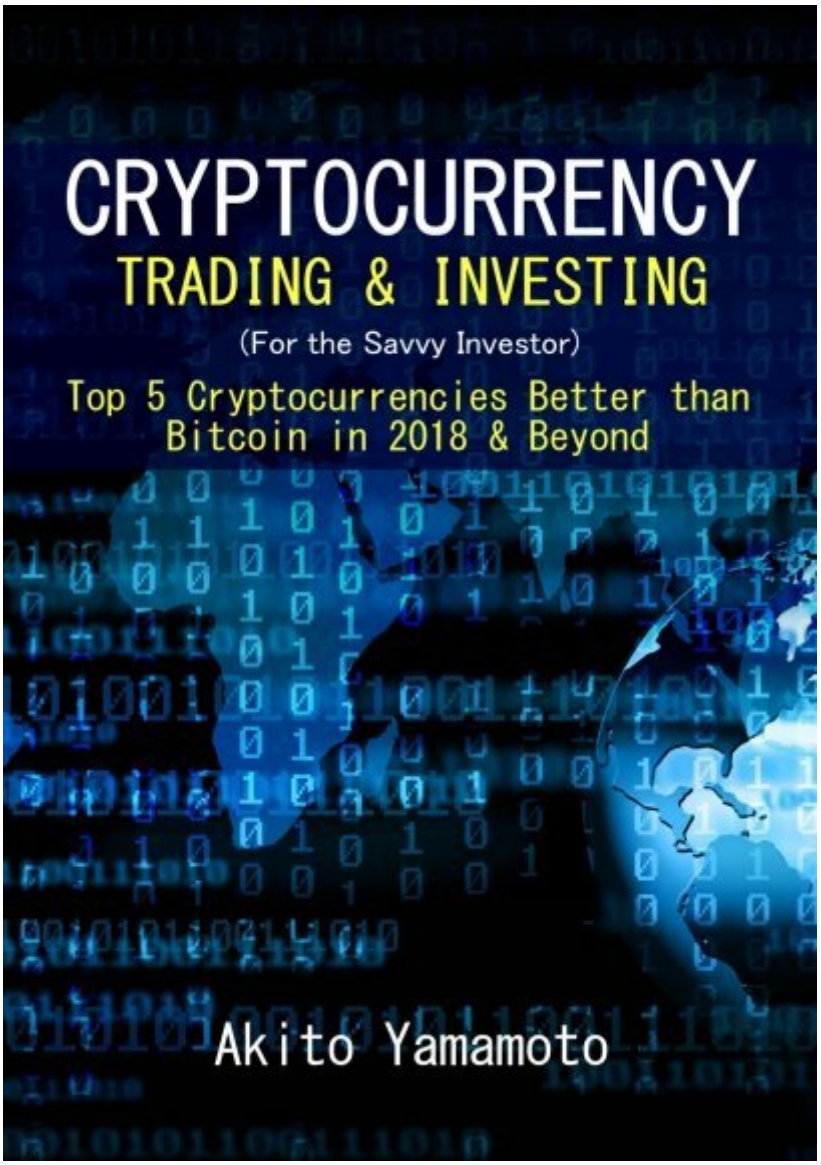
I hope that you have learned, and enjoyed this information that I have shared with you today? My reasoning for sharing this with you, is not to scare you out of investing into Bitcoin, or any other Crypto for that matter. But, it is to help inform you on what is going on out there in todays world of Cryptos.

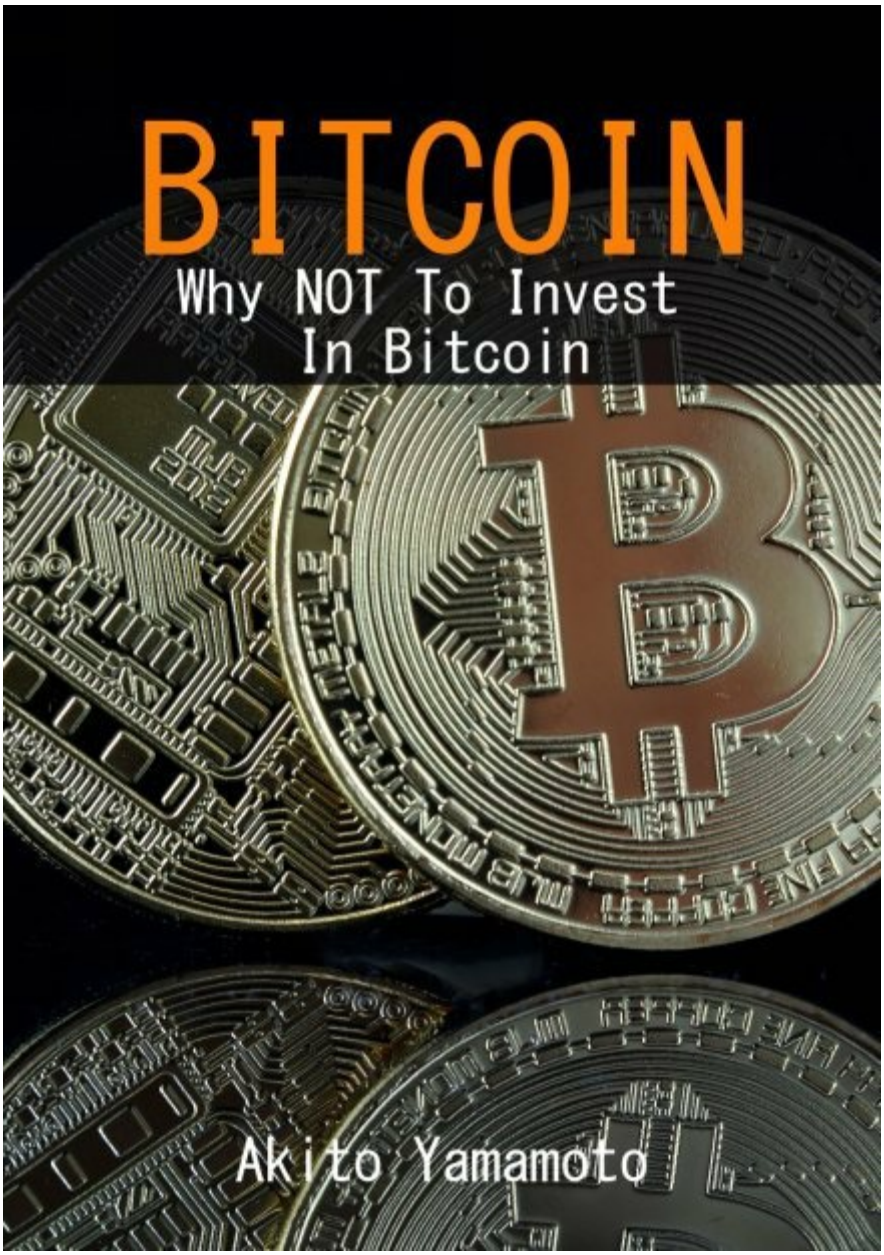
Stay educated. Stay alert. And stay a savvy investor. Always be safe, over sorry. And choose your investments wisely.

If you have time, please do me a favor & leave your reviews for this book. That would be much appreciated. And do not forget to check out other books I have written on Cryptos.

Click the image of these books, and be taken to their pages.




CRYPTOCURRENCY
TRADING & INVESTING
(For the Savvy Investor)
Top 5 Cryptocurrencies Better than Bitcoin in 2018 & Beyond
Akito Yamamoto



author does not assume and hereby disclaims any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from accident, negligence, or any other cause.