International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

# Risks associated with Cryptocurrencies

**Manish Kumar Jha**
Student
St. Josephs Degree & PG College

**Abstract**

*Cryptocurrency is a secured digital currency, which uses cryptography. A cryptocurrency is hard to forge because it is guarded using encryption. But are these cryptocurrencies future of monetary system. Every system has its benefits but also has risks involved in it. Even in cryptocurrencies we have so many risks involved in it. What are the risks involved in it. The primary target of this paper are the risks associated with cryptocurrencies. It is hoped that this study will provide a clear picture about types of risk involved in cryptocurrencies and how do they effect the system and organizations in which it is used.*

***Keywords: cryptocurrencies, risks, future, security, system.***

## I. Introduction

Cryptocurrency is a virtual currency. It is a currency, which can be used only online with cryptography, which makes it secure. Developers develop protocol using mathematics and programming to make it hard to get hacked and stop from getting duplicated. Cryptocurrencies value is totally based on the users and rules in coding. There are people who control the transaction logs and validation of bitcoins transactions, they are called Miners. Whenever a transaction is done, a record should be made of that transaction. These records are called “blockchain” here. Cryptocurrency’s technical foundations date back to the early 1980s, when an American cryptographer named David Chaum invented a “blinding” algorithm that remains central to modern web-based encryption. The algorithm allowed for secure, unalterable information exchanges between parties, laying the groundwork for future electronic currency transfers. This was known as “blinded money.”

First ever decentralized cryptocurrency was “Bitcoin”, which was created in 2009. There are so many cryptocurrencies in the market today but Bitcoin is the most popular among those all. 1 Bitcoin = 8 lakhs rupees approximately these days.

## II. How Cryptocurrency(Bitcoin) works

Cryptocurrencies rely on blockchain technology. Bitcoins are p2p decentralized currency also relies on blockchain technology.

**Person-to-person payments (P2P)** is an online technology that allows customers to transfer funds from their bank account or credit card to another individual's account via the Internet or a mobile phone. There are two general approaches for initiating a person-to-person payment:

- In the first method, based on the successful PayPal approach, users establish secure accounts with a trusted third-party vendor, designating their bank account or credit card information to be used to transfer and accept funds. Using the third party's website or mobile application, individuals can complete the process of sending or receiving funds. Users are generally identified by their email address and can send funds to anyone who is a member of the network.
- In the second method, customers use an online interface or mobile application (developed by their bank or financial institution) to designate the amount of funds to be transferred. The recipient is designated by their email address or phone number. Once the transfer has been initiated by the sender, the recipient then receives a notification to use the online interface to input his or her bank account information and routing

number to accept the transfer of funds. In this method, recipients do not need to have an account with the financial institution of the sender in order to receive a money transfer.

The blockchain is a public ledger of the currency's transactions. Public Ledger is a record of Bitcoin Transactions, which are public which can be viewed by anyone on the internet. Now let me explain what a Bitcoin Transaction is. Transfer of values between two different wallets are called Transaction. Transactions are then submitted to a public ledger and waits for confirmation. When a transaction is made, wallets use an encrypted electronic signature (an encrypted piece of data called a cryptographic signature) to provide a mathematical proof that the transaction is coming from the owner of the wallet. The confirmation process takes a bit of time (ten minutes for bitcoin) while "miners" mine (i.e. confirm transactions and add them to the public ledger). What miners do is confirm the transactions and add these transactions in public ledger. In order to add a transaction in a ledger a miner must solve a complex computational problem which is like a mathematical puzzle. As mining is open source anyone can try it. But the because of its complexity and blockchain, no one individual can do easily add or change a block at will. Cryptocurrency uses a system of cryptography (AKA encryption) to control the creation of coins and to verify transactions. The total number of Bitcoins that will be issued is capped at 21 million. The Bitcoin "mining"3 process presently creates 25 Bitcoins every 10 minutes (the number created will be halved every four years), so that limit will not be reached until the year 2140. While Bitcoin critics argue that the maximum limit is not large enough, supporters maintain that since each Bitcoin is divisible to eight decimal places, the number of fractional Bitcoins (called "satoshis") – at 21 x 1014 – will be more than enough for all conceivable applications. Conventional currencies, on the other hand, can be issued without limit.

## III. Risks associated with Cryptocurrency

1. Not every country is legally allowing anyone to invest in cryptocurrencies. So, if a person is investing or buying cryptocurrencies and if government of that country is planning to ban it then the person will be losing a ton lot of money. Bolivia, Ecuador, Kyrgyzstan, Bangladesh, Nepal and Morocco has declared Bitcoins as illegal. China is planning to ban Bitcoin and develop its own digital currency. Many of the countries are planning to ban cryptocurrencies after the attacks of Ransomware.
2. Cryptocurrencies are exchanged online by E-wallet. So, if a person is buying it from an unknown wallet service provider then it is a risk. Wallet provider can spam them. Recently Google has banned three fake Bitcoin wallets. This kind of incidents risks the use of Bitcoins.
3. Once you have transferred some amount to an address then transactions cannot be cancelled or reversed.
4. Bitcoin is purely digital existence, newness, and technical complexity are large hurdles for most people. A lot of people (especially older generations) struggle with the fact that you can't hold a Bitcoin in your hands.
5. A single file on Bitcoin user's computer can risk his computers security and which can lead to easy access to the bitcoins he holds in his wallet.
6. Criminals can use this currency to keep themselves safe from the government. So, cryptocurrencies are also a risk for the government officials.
7. Forgotten or lost passwords leading to inability to access the funds which were invested. A guy lost his hard drive with keys for 7500 Bitcoins.
8. No single cryptocurrency can be trusted as one could be superseded by another technology that is perceived to be superior (we are seeing evidence of this play out with the rise of Ethereum). Reportedly Major tech companies are working together and investing in Ethereum, such as Microsoft and Intel and also investment banks like JP Morgan.
9. Quantum computing could break the encryption that underpins the security of the network.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

## IV. Threats and Attacks from using Cryptocurrencies

Ransomware attacks will force users to buy cryptocurrency. Cybercriminals will continue to demand ransoms in cryptocurrency, because of the unregulated and almost anonymous cryptocurrency market: there is no need to share any data with anyone, no one will block the address, no one will catch you, and there is little chance of being tracked. At the same time, further simplification of the monetization process will lead to the wider dissemination of encryptors.

Fall of ICO (Initial Coin Offering). ICO means crowdfunding via cryptocurrencies. 2017 saw tremendous growth of this approach; with more than $3 billion collected by different projects, most related in some way to blockchain. Next year we should expect ICO-hysteria to decline, with a series of failures (inability to create the ICO-funded product), and more careful selection of investment projects. Many unsuccessful ICO projects may negatively affect the exchange rate of cryptocurrencies (Bitcoin, Ethereum etc.), which in 2017 experienced unprecedented growth.

James Howells, an IT worker from Newport, claims to have unintentionally dumped 7,500 bitcoins in mid-2013. The value of the cryptocurrency was around $130 at the time Howells claims to have thrown the hard drive away. It is currently worth $11,350 (Rs. 726602).

More than $300m of cryptocurrency has been lost after a series of bugs in a popular digital wallet service led one curious developer to accidentally take control of and then lock up the funds, according to reports.

Notpetya started as a fake Ukrainian tax software update, and went on to infect hundreds of thousands of computers in more than 100 countries over the course of just a few days. This ransomware is a variant of Petya, but uses the same exploit behind WannaCry. It hit several firms in the US and caused major financial damage: For example, the attack cost pharmaceutical giant Merck more than $300 million in Q3 alone, and is on track to hit that amount again in Q4.

WannaCry attack began on Friday, 12 May 2017, with evidence pointing to an initial infection in Asia at 7:44am UTC. The initial infection was likely through an exposed vulnerable SMB port, rather than email phishing as initially assumed. Within a day was reported to have infected more than 230,000 computers in over 150 countries.

Locky is currently the top payload in terms of ransomware and across all malware families, according to a report from security firm Proofpoint. While Locky was 2016's most popular ransomware strain, new variants called Diablo and Lukitus also surfaced this year, using the same phishing email attack vector to initiate their exploits.

On October 24, 2017, some users in Russia and Ukraine reported a new ransomware attack, named "Bad Rabbit", which follows a similar pattern to WannaCry and Petya by encrypting the user's file tables and then demands a Bitcoin payment to decrypt them. ESET believed the ransomware to have been distributed by a bogus update to Adobe Flash software. Among agencies that were affected by the ransomware included Interfax, Odessa International Airport, Kiev Metro, and the Ministry of Infrastructure of Ukraine. As it used corporate network structures to spread, the ransomware was also discovered in other countries, including Turkey, Germany, Poland, Japan, South Korea, and the United States. Experts believed the ransomware attack was tied to the Petya attack in the Ukraine, though the only identity to the culprits are the names of characters from the *Game of Thrones* series embedded within the code.

Recently three fake Bitcoin wallets were found in Google Play store. These apps pretended to be legitimate bitcoin wallets, but instead were fake. Apps were designed to trick sellers to provide the attacker's bitcoin address (not the legitimate seller's) to buyers so payments would go to the attacker, according researchers. Collectively the three apps were downloaded 20,000 times by users. The apps were identified as "**Bitcoin mining**", "**Blockchain Bitcoin Wallet – Fingerprint**" and "**Fast Bitcoin Wallet**."

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

## V. How to be safe when dealing with Cryptocurrencies

1. When buying Bitcoin or investing in Bitcoin be careful with the provider or wallet you're buying from. Even if you're investing in Bitcoin analyze the market before investing because if you're investing small amount then you can lose more than 50% of your investment or can lose all of it.
2. Always double check the address to which you're going to transfer Bitcoins. Since the beginning of the Bitcoins many of the users have mistakenly transferred Bitcoins to some other address.
3. Always keep your system updated and use a popular anti-virus which can keep your computer safe from any type of attacks. This way you can save your Bitcoin wallets and information regarding the Bitcoins.
4. Always save your passwords from somewhere from where it cannot be stolen. This way you can always access your wallets or online profiles even when you forgot your passwords. Also try to link your wallets with your primary E-mail accounts.
5. Don't be lazy to check the market and try to check whether the currency you've invested in is doing well in the market or not. This way you can plan.

## VI. List of most popular cryptocurrencies present in the market

There are around 1378 cryptocurrencies in the world. But not all of them are secured and useful for the common people.

Following are currently the top 10 cryptocurrencies in the market.

| S. No | Cryptocurrency Name | Market Value | Circulating Supply | Acronym |
|---|---|---|---|---|
| **1.** | Bitcoin | ₹.895559 | 16760487 | BTC |
| **2.** | Ethereum | ₹.47122 | 96540529 | ETH |
| **3.** | Bitcoin Cash | ₹.181362 | 16873238 | BCH |
| **4.** | Ripple | ₹.63 | 38739144847 | XRP |
| **5.** | Litecoin | ₹.17652 | 54450483 | LTC |
| **6.** | Cardano | ₹.25 | 25927070538 | ADA |
| **7.** | IOTA | ₹.242 | 2779530283 | MIOTA |
| **8.** | Dash | ₹.77888 | 7772352 | DASH |
| **9.** | NEM | ₹.62 | 8999999999 | XEM |
| **10.** | Bitcoin Gold | ₹.19674 | 16724449 | BTG |

## VII. Influential People thoughts on Cryptocurrencies

Bill Gates 18 time world's richest person said, "Bitcoin is exciting because it shows how cheap it can be. Bitcoin is better than currency in that you don't have to be physically in the same place and, of course, for large transactions, currency can get pretty inconvenient."

Warren Buffet CEO of Berkshire Hathaway and one of the richest persons in the world said, "The idea that it [bitcoin] has some huge intrinsic value is just a joke in my view."

Dr. Eric Schmidt is an American software engineer, a businessman, and the Executive Chairman of Alphabet Inc. and was ranked as the 119$^{th}$ richest person in the world, with an estimated wealth of US$11.1 billion. He once said, "Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value".

Richard Branson, an English businessman and investor who is best known as the founder of Virgin Group comprising more than 400 companies. Branson is the seventh richest citizen of the United Kingdom, with an estimated net worth of US$4.9 billion. He mentioned that, "There's a big industry around and, you know people have made fortune out of bitcoin."

Peter Theil, Co-Founder of PayPal and investor in Bitcoin merchant processor Bitpay. He says, "I do think Bitcoin is the first [encrypted money] that has the potential to do something like change the world."

Julian Assange the founder of WikiLeaks said, "Bitcoin actually has the balance and incentives right, and that is why it is starting to take off."

You likely know Tyler and Cameron Winklevoss, who tried and failed to gain control of Facebook after alleging that it had been appropriated from them, thanks to Armie Hammer's satirical portrayal of both siblings in *The Social Network*. But the Winklevii have a second act in their enormous Bitcoin investment. While they were shut out of creating a Bitcoin exchange traded fund (ETF), their 2013 investment in $11 million worth of Bitcoin (which reportedly amounted to one percent of all the currency in circulation) looks pretty rosy now. That same amount is worth approximately 21 times as much now, putting their total at about $231 million.

Tim Draper, worth billions, thanks in part to his early investment in Skype, made headlines for his purchase of 30,000 Bitcoins in 2014 from that same government auction. Then worth about $19 million, that stash would be up to $171 million now. Draper is clearly feeling optimistic about the digital currency market, as he's gone on to back Tezos, a new cryptocurrency.

Satoshi Nakamoto is the shadowy figure sitting at the heart of Bitcoin, which itself still confounds so many. After inventing Bitcoin with a 2008 white paper describing a software tied to digital currency, Nakamoto retreated from public life. People aren't even sure if that is his (or her) real name. While one man came forward to say he was Nakamoto, online sleuths disputed the evidence. Theories abound as to who Nakamoto really is, but it's clear they have a whole lot of Bitcoins at their disposal. A Bitcoin developer estimated in 2013 that Nakamoto had around 1 million Bitcoins. At a valuation of about $6,133 as of this writing, that would be theoretically worth an astounding $6.1 billion. A huge caveat here, though: If Nakamoto were to start selling off their entire supply of Bitcoin, it would rapidly drive down demand for the currency, and therefore the value of the holding.

Tony Gallippi is the cofounder and chairman of Bitpay, currently the leading Bitcoin processor, and is said to be among the largest holders of the currency. While he hasn't disclosed the exact value of his Bitcoin investments, estimates have put it around $20 million.

## VIII. Conclusion

Since 2009 the price of Bitcoin a kind of cryptocurrency has been increasing drastically. It costs around 90lakh rupees presently which makes it the costliest cryptocurrency in the world and attracts investors. This attracts not only old players but also new investors to invest in these currencies. As people are getting involved with these currencies, the security of these currencies is also at risk. There are so many threats when dealing with cryptocurrencies. But if an individual or a body is cautioned in using these currencies, it can lead to a great profit for them. Today so many people have gained a high income from investing in cryptocurrencies just because of taking decisions wisely and with caution.

## IX. References


- The top 10 worst ransomware attacks of 2017, so far - TechRepublic. (2017, November 01). Retrieved December 25, 2017, from http://www.mytopposts.com/cyber-security/top-10-worst-ransomware-attacks-2017-far-techrepublic
- Maxwell, S. (n.d.). Public Ledger. Retrieved December 25, 2017, from https://cryptocurrencymadesimple.com/public-ledger/
- DeMichele, T. (n.d.). How Does Cryptocurrency Work? Retrieved December 25, 2017, from http://cryptocurrencyfacts.com/how-does-cryptocurrency-work-2/
- Cryptocurrency Market Capitalizations. (n.d.). Retrieved December 25, 2017, from https://coinmarketcap.com/
- Momoh, O. (2017, September 05). Initial Coin Offering (ICO). Retrieved December 25, 2017, from https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp
- Person-to-Person Payments (P2P). (n.d.). Retrieved December 25, 2017, from http://www.investinganswers.com/financial-dictionary/personal-finance/person-person-payments-p2p-2584