International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 4 Issue: 2 March-April 2018 p-ISSN: 2394-8280

SURVEY PAPER ON CRYPTO CURRENCY BIT COIN

Mr. Yeshwant Maheshram[1], Mr. Siddharth Singhai[2]

Research Analyst, Corpus Medisol Solution Private Limited, Indore 1
BE, Medicaps Institute of Science & Technology, Indore 2, Yeshsap@lcmass.com

1. INTRODUCTION

Bitcoin is a new currency that was created in 2009 by an unknown person using the alias Satoshi Nakamoto. Transactions are made with no middle men – meaning, no banks! Bitcoin can be used to book hotels on Expedia, shop for furniture on Overstock and buy Xbox games. But much of the hype is about getting rich by trading it. The price of bitcoin skyrocketed into the thousands in 2017. Bitcoins can be used to buy merchandise anonymously. In addition, international payments are easy and cheap because bitcoins are not tied to any country or subject to regulation. Small businesses may like them because there are no credit card fees. Some people just buy bitcoins as an investment, hoping that they'll go up in value. Many marketplaces called "bitcoin exchanges" allow people to buy or sell bitcoins using different currencies. Coin base is a leading exchange, along with Bitstamp and Bitfinex. But security can be a concern: bitcoins worth tens of millions of dollars were stolen from Bitfinex when it was hacked in 2016. People can send bitcoins to each other using mobile apps or their computers. It's similar to sending cash digitally. People compete to "mine" bitcoins using computers to solve complex math puzzles. This is how bitcoins are created. Currently, a winner is rewarded with 12.5 bitcoins roughly every 10 minutes. Bitcoins are stored in a "digital wallet," which exists either in the cloud or on a user's computer. The wallet is a kind of virtual bank account that allows users to send or receive bitcoins, pay for goods or save their money. Unlike bank accounts, bitcoin wallets are not insured by the FDIC. Though each bitcoin transaction is recorded in a public log, names of buyers and sellers are never revealed – only their wallet IDs. While that keeps bitcoin users' transactions private, it also lets them buy or sell anything without easily tracing it back to them. That's why it has become the currency of choice for people online buying drugs or other illicit activities. . No one knows what will become of bitcoin. It is mostly unregulated, but some countries like Japan, China and Australia have begun weighing regulations. Governments are concerned about taxation and their lack of control over the currency.

2. HOW DO BIT COINS WORKS:

Bitcoin – the initial virtual banking currency of the internet – has existed for several years now and many people have questions about them. Where do they come from? Are they legal? Where can you get them? Why did they split into Bitcoin and Bitcoin Cash? Here are the basics you need to know.

Crypto currency Defined

Crypto currencies are just lines of computer code that hold monetary value. Those lines of code are created by electricity and high-performance computers.Crypto currency is also known as digital currency. Either way, it is a form of digital public money that is created by painstaking mathematical computations and policed by millions of computer users called 'miners'. Physically, there is nothing to hold although you can exchange crypto for cash.'Crypto' comes from the word cryptography, the security process used to protect transactions that send the lines of code out for purchases. Cryptography also controls the creation of new 'coins', the term used to describe specific amounts of code. There are literally hundreds of coins now; only a handful have the potential to become a viable investment.Governments have no control over the creation of crypto currencies, which is what initially made them so popular. Most crypto currencies begin with a market cap in mind, which means that their production will decreae over time thus, ideally, making any particular coin more

valuable in the future . Bitcoin was the first crypto coin currency ever invented. No one knows exactly who created it – crypto currencies are designed for maximum anonymity – but bit coins first appeared in 2009 from a developer supposedly named Satoshi Nakamoto. He has since disappeared and left behind a Bit coin fortune.

Because Bit coin was the first crypto currency to exist, all digital currencies created since then are called Altcoins, or alternative coins. Litecoin, Peercoin, Feathercoin, Ethereum and hundreds of other coins are all Altcoins because they are not Bitcoin.

One of the advantages of Bitcoin is that it can be stored offline on a person's local hardware. That process is called cold storage and it protects the currency from being taken by others. When the currency is stored on the internet somewhere (hot storage), there is high risk of it being stolen.

On the flip side, if a person loses access to the hardware that contains the bitcoins, the currency is simply gone forever. It's estimated that as much as $30 billion in bitcoins have been lost or misplaced by miners and investors. Nonetheless, Bitcoins remain incredibly popular as the most famous cryptocurrency over time.

3. Why Bitcoins Are So Controversial

Various reasons have converged to make Bitcoin currency a real media sensation. From 2011-2013, criminal traders made bitcoins famous by buying them in batches of millions of dollars so they could move money outside of the eyes of law enforcement. Subsequently, the value of bitcoins skyrocketed. Scams, too, are very real in the crypto currency world. Naive and savvy investors alike can lose hundreds or thousands of dollars to scams.Ultimately, though, bitcoins and altcoins are highly controversial because they take the power of making money away from central federal banks, and give it to the general public. Bitcoin accounts cannot be frozen or examined by tax men, and middleman banks are completely unnecessary for bitcoins to move. Law enforcement and bankers see bitcoins as 'gold nuggets in the wild, wild west', beyond the control of traditional police and financial institutions.

4. How Bitcoins Work

Bitcoins are completely virtual coins designed to be 'self-contained' for their value, with no need for banks to move and store the money.Once you own bitcoins, they behave like physical gold coins: they possess value and trade just as if they were nuggets of gold in your pocket. You can use your bit coins to purchase goods and services online, or you can tuck them away and hope that their value increases over the years.Bitcoins are traded from one personal 'wallet' to another. A wallet is a small personal database that you store on your computer drive (i.e cold storage), on your smartphone, on your tablet, or somewhere in the cloud (hot storage).For all intents, bitcoins are forgery-resistant. It is so computationally-intensive to create a bitcoin, it isn't financially worth it for counterfeiters to manipulate the system.

5. Bitcoin Values and Regulations

A single bitcoin varies in value daily; you can check places like Coindesk to see today's value. There are more than two billion dollars worth of bitcoins in existence. Bitcoins will stop being created when the total number reaches 21 billion coins, which will be sometime around the year 2040. As of 2017, more than half of those bitcoins had been created.

Bitcoin currency is completely unregulated and completely decentralized. There is no national bank or national mint, and there is no depositor insurance coverage. The currency itself is self-contained and un-collateraled, meaning that there is no precious metal behind the bitcoins; the value of each bitcoin resides within each bitcoin itself.Bitcoins are stewarded by 'miners', the massive network of people who contribute their personal computer to the Bitcoin network.

Miners act as a swarm of ledger keepers and auditors for Bitcoin transactions. Miners are paid for their accounting work by earning new bitcoins for each week they contribute to the network.

6. How Bitcoins Are Tracked

A Bitcoin holds a very simple data ledger file called a blockchain. Each blockchain is unique to each individual user and his/her personal bitcoin wallet.
All bitcoin transactions are logged and made available in a public ledger, helping ensure their authenticity and preventing fraud. This process helps to prevent transactions from being duplicated and people from copying bitcoins.
Note: While every Bitcoin records the digital address of every wallet it touches, the bitcoin system does NOT record the names of the individuals who own wallets. In practical terms, this means that every bitcoin transaction is digitally confirmed but is completely anonymous at the same time.
So, although people cannot easily see your personal identity, they can see the history of your bitcoin wallet. This is a good thing, as a public history adds transparency and security, helps deter people from using bitcoins for dubious or illegal purposes.

7. Banking or Other Fees to Use Bitcoins

There are very small fees to use bitcoins. However, there are no ongoing banking fees with bitcoin and other cryptocurrency because there are no banks involved. Instead, you will pay small fees to three groups of bitcoin services: the servers (nodes) who support the network of miners, the online exchanges that convert your bitcoins into dollars, and the mining pools you join.
The owners of some server nodes will charge one-time transaction fees of a few cents every time you send money across their nodes, and online exchanges will similarly charge when you cash your bitcoins in for dollars or euros. Additionally, most mining pools will either charge a small one percent support fee or ask for a small donation from the people who join their pools.
In the end, while there are nominal costs to use Bitcoin, the transaction fees and mining pool donations are much cheaper than conventional banking or wire transfer fees.

Bitcoin Production Facts

Bitcoins can be 'minted' by anyone in the general public who has a strong computer. Bitcoins are made through a very interesting self-limiting system called cryptocurrency mining and the people who mine these coins are called miners. It is self-limiting because only 21 million total bitcoins will ever be allowed to exist, with approximately 11 million of those Bitcoins already mined and in current circulation.
Bitcoin mining involves commanding your home computer to work around the clock to solve 'proof-of-work' problems (computationally-intensive math problems). Each bitcoin math problem has a set of possible 64-digit solutions. Your desktop computer, if it works nonstop, might be able to solve one bitcoin problem in two to three days, likely longer.
For a single personal computer mining bitcoins, you may earn perhaps 50 cents to 75 cents USD per day, minus your electricity costs.
For a very large-scale miner who runs 36 powerful computers simultaneously, that person can earn up to $500 USD per day, after costs.
Indeed, if you are a small-scale miner with a single consumer-grade computer, you will likely spend more in electricity that you will earn mining bitcoins. Bitcoin mining is only really profitable if you run multiple computers, and join a group of miners to combine your hardware power. This very prohibitive hardware requirement is one of the biggest security measures that deters people from trying to manipulate the Bitcoin system.

8. Bitcoin Security

They are as secure as possessing physical precious metal. Just like holding a bag of gold coins, a person who takes reasonable precautions will be safe from having their personal cache stolen by hackers.As mentioned earlier, your bitcoin wallet can be stored online (i.e. a cloud service) or offline (a hard drive or USB stick). The offline method is more hacker-resistant and absolutely recommended for anyone who owns more than 1 or 2 bitcoins but it is not without risk.

More than hacker intrusion, the real loss risk with bitcoins revolves around not backing up your wallet with a failsafe copy. There is an important .dat file that is updated every time you receive or send bitcoins, so this .dat file should be copied and stored as a duplicate backup every day you do bitcoin transactions.

Security note: The collapse of the Mt.Gox bitcoin exchange service was not due to any weakness in the Bitcoin system. Rather, that organization collapsed because of mismanagement and their unwillingness to invest any money in security measures. Mt.Gox, for all intents and purposes, had a large bank with no security guards, and it paid the price.

9. Abuse of Bitcoins

There are currently three known ways that bitcoin currency can be abused.

1) Technical weakness – time delay in confirmation: bitcoins can be double-spent in some rare instances during the confirmation interval. Because bitcoins travel peer-to-peer, it takes several seconds for a transaction to be confirmed across the P2P swarm of computers. During these few seconds, a dishonest person who employs fast clicking can submit a second payment of the same bitcoins to a different recipient.While the system will eventually catch the double-spending and negate the dishonest second transaction, if the second recipient transfers goods to the dishonest buyer before they receive confirmation, then that second recipient will lose both the payment and the goods.

2) Human dishonesty – pool organizers taking unfair share slices: Because bitcoin mining is best achieved through pooling (joining a group of thousands of other miners), the organizers of each pool get the privilege of choosing how to divide up any bitcoins that are discovered. Bitcoin mining pool organizers can dishonestly take more bitcoin mining shares for themselves.

3) Human mismanagement – online exchanges: With Mt. Gox being the biggest example, the people running unregulated online exchanges that trade cash for bitcoins can be dishonest or incompetent. This is the same as Fannie Mae and Freddie Mac investment banks going under because of human dishonesty and incompetence. The only difference is that conventional banking losses are partially insured for the bank users, while bitcoin exchanges have no insurance coverage for users.

10. Four Reasons Why Bitcoins Are Such a Big Deal

There is a lot of controversy around bitcoins. These are the top reasons why:

1) Bitcoins are not created by any central bank, nor regulated by any government. Accordingly, there are no banks logging your money movement, and government tax agencies and police cannot track your money. This is bound to change eventually, as unregulated money is a real threat to government control, taxation, and policing.

Indeed, bitcoins have become a tool for contraband trade and money laundering, precisely because of the lack of government oversight. The value of bitcoins skyrocketed in the past because wealthy criminals were purchasing bitcoins in large volumes. Because there is no regulation, however, you can lose out immensely as a miner or investor.

2) Bitcoins completely bypass banks. Bitcoins are transferred via a peer-to-peer network between individuals, with no middleman bank to take a slice.

Bitcoin wallets cannot be seized or frozen or audited by banks and law enforcement. Bitcoin wallets cannot have spending and withdrawal limits imposed on them. For all intents: nobody but the owner of the bitcoin wallet decides how their wealth will be managed.

11. This is really threatening to banks, as you might guess.

3)Bitcoins are changing how we store and spend our personal wealth. Since the advent of printed (and eventually virtual) money, the world has handed over the power of currency to a central mint and various banks. These banks print our virtual money, store our virtual money, move our virtual money,

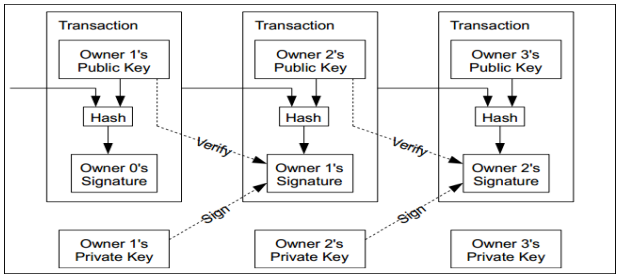
and charge us for their middleman services.
If banks need more currency, they simply print more or conjure more digits in their electronic ledgers. This system is easily abused and gamed by banks because paper money is essentially paper checks with a promise to have value, with no actual physical gold behind the scenes to back those promises.
Bitcoins are designed to put the control of personal wealth back into the hands of the individual. Instead of paper or virtual bank balances that promise to have value, Bitcoins are actual packages of complex data that have value in them.
4) Bitcoin transactions are irreversible. Conventional payment methods, like a credit card charge, bank draft, personal checks, or wire transfer, do have the benefit of being insured and reversible by the banks involved. In the case of bitcoins, every time bitcoins change hands and change wallets, the result are final. Simultaneously, there is no insurance protection of your bitcoin wallet: If you lose your wallet's hard drive data or even your wallet password, remember: your wallet's contents are gone forever.

12. How Are Bitcoins Spent?

In layman's terms: Imagine you're buying a Coke at the supermarket with a debit card. The transaction has three elements: your card, corresponding to your bank account and your money, the bank itself that verifies the transaction and the transfer of money, and the store that accepts the money from the bank and finalizes the sale. A Bitcoin transaction has, broadly speaking, the same three components.

Each Bitcoin user stores the data that represents his or her amount of coins in a program called a wallet, consisting of a custom password and a connection to the Bitcoin system. The user sends a transaction request to another user, buying or selling, and both users agree. The peer-to-peer Bitcoin system verifies the transaction via the global network, transferring the value from one user to the next and inserting cryptographic checks and verification at many levels. There is no centralized bank or credit system: the peer-to-peer network completes the encrypted transaction with the help of Bitcoin miners.

The advanced explanation: The technical side of things is a bit more complex. Each new Bitcoin transaction is recorded and verified onto a new block of data in the blockchain. (The two parties in the exchange are represented by randomized numbers that make each transaction essentially anonymous, even as they're being verified.) Each block in the chain includes cryptological code linking it to and verifying it for the previous block.



In the conventional sense, Bitcoin transactions are incredibly secure. Thanks to complex cryptography at every step in the process, which can take quite a lot of time to verify (see below), it's more or less i mpossible to fake a transaction from one person or organization to another. However, it is possible to

"steal" bitcoins by discovering someone's digital wallet and the password that they use to access it. If that information is found, via hacking or social engineering, a digital Bitcoin stash can dispensary wit hout any way to trace the thief. Since Bitcoin isn't regulated or secured in the same way your bank ac count or credit account is, that money is simply gone.

12. Bitcoin Weaknesses

So if Bitcoin is so great, why isn't everyone using it? Well, obviously, it has some drawbacks too, especially at the current time.

Possible Government Interference

Any time something new comes around and challenges the status quo, the government is going to get involved to make sure that things remain the way they are *supposed* to be. The fact is that the US government, and other governments, are looking into Bitcoin for a variety of reasons. Just in the last few days, the US government has started seizing some accounts from the biggest Bitcoin exchange. More is likely to come in the future.

No Monetary Sovereignty

Perhaps the biggest weakness of bitcoin is that it is not a "recognized" sovereign currency—that is, it is not backed by the full faith of any governing body. While this could be seen as strength, the fact that Bitcoin is a fiat currency which is accepted only on the perceived value of other bitcoin users makes it highly vulnerable to destabilization. Simply put, if one day a large number of merchants who accept bitcoin as a form of payment stop doing so, then the value of bitcoin would fall drastically.

The current high value of Bitcoin is a function of both the relative scarcity of Bitcoins themselves and its popularity as a means of investment and wealth generation. If confidence in the Bitcoin market is suddenly and drastically reduced—for example, if a major government declared Bitcoin use illegal, or one of the largest Bitcoin exchanges was hacked and lost all of its stored value—the value of the currency will crash and investors will lose huge amounts of money.

The United States Treasury does not recognize bitcoin as a conventional currency, but does recognize its status as a commodity, like stocks and bonds. Similarly, the US Internal Revenue Service considers bitcoins property and taxes them as such if they are declared. No other country has declared bitcoin to be a recognized currency, but engagement with bitcoin and other cryptocurrencies varies from place to place. Some countries are investigating bitcoin as a growing commodity market, some take the same stance as the US declaring them assets, and some have explicitly banned their use for transfer of goods or services (though the means of enforcing those bans are limited).

Lack of Protections

The Bitcoin network has no built-in protection mechanisms when it comes to accidental loss or theft. For instance, if you lose the hard drive where your Bitcoin wallet file is stored (think corruption or

drive failure with no backup), the Bitcoins held in that wallet are lost forever to the entire economy. Interestingly, this is an aspect which further exacerbates the limited supply of Bitcoins.

Additionally, if your wallet file is stolen or compromised and the Bitcoins contained within it are spent by the thief before the rightful owner, the double spending protection mechanism built into the network means the rightful owner has no recourse. Unlike if, for example, your credit card is stolen, you can call the bank and cancel the card, bitcoin has no such authority. The Bitcoin network only knows that the bitcoins in the compromised wallet file are valid and processes them accordingly. In fact, there is already malware out there which is designed specifically to steal Bitcoins.

Bitcoin markets are vulnerable to attack or fraud. Major exchanges like GBH and Cryptsy have been shut down with all the Bitcoin entrusted to their care presumably stolen by the operators. Japan-based Mt. Gox, formerly the handler of over half the Bitcoin transactions on the planet, was shuttered after a theft of hundreds of thousands of Bitcoins. The 2014 incident caused a huge (but temporary) drop in the value of Bitcoin worldwide.

Limited Concurrent Transactions

The Bitcoin block system requires connection and confirmation from the peer-to-peer network to be verified. Because each block contains a limited record of transactions and an upper limit to the amount of new transactions that can be written, there's a limit to how many people can buy and sell with the system at any given time. As more and more vendors and individuals use Bitcoin to do business, the number of transactions per second increase, and the peer-to-peer network is becoming congested, with some operations without transaction fees taking hours to clear. Whereas conventional payment systems like credit cards can simply expand their connections and processing power to speed up processing, the isolated peer-to-peer nature of bitcoin doesn't allow it to scale with the global financial system.

Black Market Appeal

A central principle to the design of the Bitcoin system is that there is no single transactional processing authority. As a result, no single user can be locked out of the system. Combine this with the inherent anonymity of transactions, and you have an ideal medium of exchange for nefarious purposes.

Bitcoin has become an ideal means for commerce in illicit goods and services. The quintessential case is the Silk Road, a dark web site that allowed users to anonymously trade items like drugs and fake identification, all bought with Bitcoin thanks to its untraceable nature. The story of Silk Road's illegal trade didn't even stop after the US Drug Enforcement Agency and Department of Justice shut down the site and seized its digital holdings in 2013. A Secret Service agent was charged with stealing over $800,000 of bitcoin from the investigators, who had held the seized digital currency to be auctioned off for the benefit of the law enforcement agencies.

While this is not exactly a weakness in Bitcoin (after all, drug dealers using cash doesn't undermine the value of the currency itself), the unintended consequence of its usage for dubious purposes could be considered one. In fact, the US Treasury Department recently applied money laundering rules to bitcoin exchanges.

Subjects of Debate and Controversy

Lastly, let's indulge a bit of controversy surrounding Bitcoin. While these topics of conversation are interesting, most everything in this section is conjecture and should be taken with a grain of salt—we just think they're worth noting to get a full picture of the Bitcoin story.

Enigmatic Developer

The primary designer of the bitcoin specification is a "person" named Satoshi Nakamoto. Person is put in quotes here because Nakamoto has not connected "his" identity with a publicly known person. Satoshi Nakamoto could be an individual man or woman, an internet handle, or a group of people, but nobody actually knows. Once their work of designing the Bitcoin network was complete, this person or persons essentially disappeared.

Multiple individual people and teams of developers have been theorized to be the "real" Satoshi Nakamoto, with no conclusive proof for any one of them at the time of writing. Whoever he, she, or they are, Satoshi Nakamoto is estimated to be in possession of billions of US dollars worth of Bitcoin at current market rates.

Resistance From Conventional Investors

Many experts in standard money markets and investments consider Bitcoin a poor choice for investing money. The extreme volatility of Bitcoin versus investments like stocks, bonds, and standard commodities makes larger and older institutions wary. In addition, some investors and investigators consider Bitcoin and other cryptocurrencies to be either a passing fad (an economic bubble) and thus an extremely risky means of investment, or a fraud in and of itself, a "Ponzi scheme" for the benefit of Satoshi Nakamoto and other early investors.

On the other hand, it's possible that some of these statements are made specifically to manipulate the value of Bitcoin: JP Morgan Chase has been accused of publicly calling the worth of Bitcoin into question via CEO statements while investing in it at the same time. As stated above, use caution when dealing in Bitcoin either as a means of purchasing goods or services or investing.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.
[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with mini mal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.
[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3 , no 2, pages 99-111, 1991.
[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamp ing," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1 993.
[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conferen ce on Computer and Communications Security, pages 28-35, April 1997.
[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashc ash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.
[8] W. Feller, "An introduction to probability theory and its applications," 1957.