2nd International Conference on Recent Innovations in Management and Engineering
IIMT College of Engineering, Greater Noida
24th June 2017, www.conferenceworld.in
(ICRIME-17)
ISBN: 978-93-86171-50-4

THE DAWN OF DIGITAL CURRENCY- BITCOIN

Jyotsna Oberoi

Student, M.COM , Kurukshetra University , UGC-NET (JRF)

ABSTRACT

Bitcoin is a form of digital currency, created and held electronically. No one controls it. Bitcoins aren't printed, like dollars or euros – they're produced by people, and increasingly businesses, running computers all around the world, using software that solves mathematical problems. Bitcoin has emerged as the most successful cryptographic currency in history. Within two years of its quiet launch in 2009, Since then a growing literature has identified hidden-but-important properties of the system, discovered attacks, proposed promising alternatives, and singled out difficult future challenges. Meanwhile a large and vibrant open-source community has proposed and deployed numerous modifications and extensions. Unlike traditional payment systems, which transfer funds denominated in sovereign currencies, Bitcoin has its own metric for value called bitcoin (with lowercase letter "b", and abbreviated as BTC1). Bitcoin is a complex scheme, and its implementation involves a combination of cryptography, distributed algorithms, and incentive driven behaviour. Moreover, recent developments suggest that Bitcoin operations may involve risks whose nature and proportion are little, if at all, understood. In light of these considerations, the purpose of this paper is to give the reader a reliable abbreviated overview of Bitcoin and its usage. This article is a short history of Bitcoin.

Keywords: Bitcoin, Digital Currency, Dollars

I. INTRODUCTION

Bitcoin is a digital currency system that enables participants to create and transfer bitcoins using a blockchain which are the rails upon which the bitcoins are created and transferred. Bitcoin is a peer-to-peer currency. Peer-to-peer means that no central authority issues new money or tracks transactions. These tasks are managed collectively by the network. Bitcoin prices in the last one year have only headed north. In the last five months since January 2017, the value of BTC has doubled in absolute value compared to the dollar. Bitcoin is a digital currency as opposed to physical currency that we're accustomed to and use in our daily life. Straight off their site, Bitcoin is described as a pseudo-anonymous, P2P technology operating with no central authority or banks, it's open-source, public, owned by no one and open for everybody to take part; but what does that all mean? "Bitcoin is the leader in a new generation of emerging currencies known as "cryptocurrencies" which aim to, among other things, facilitate the movement of money electronically while still maintaining a sense of privacy," Bitcoin stores no personal data (a characteristic we will later see as a double-edged sword) and therefore nothing personally identifiable is recorded. Instead, if you were to have a Bitcoin, you'd have many wallet addresses, which essentially are hashes of public keys. Bitcoin has no way of identifying how much you own or spend however there exists a "blockchain" where all transactions are recorded. These transactions can be seen by everyone however nothing points back to specific users sits transactions are recorded using random numbers of

which anyone can have several. The transactions are very much like Swiss banking; you only have a number, you have no clue who is behind the number and payments are made directly to that number only.

II. OBJECTIVE OF THE STUDY

The aim of the study is :

- to give the reader a reliable abbreviated overview of Bitcoin and its usage
- To understand how current Bitcoin works and its adwantages
- To investigate the factors why bitcoins are such a big deal

III. RESEARCH METHODOLOGY

The researcher used an explorative analysis technique supported past literature from various journals, annual, reports, newspapers and magazines covering wide assortment of educational literature on bitcoins . In keeping with the objectives of the study, the analysis style is of descriptive in nature. Available secondary data was extensively used for the study.

IV. HISTORY OF BITCOIN

2008/2009: Bitcoin's birth:

In November 2008, someone going by the user name 'Satoshi Nakamoto' released a paper to a cryptography mailing list. The 9-page paper was entitled "Bitcoin: A Peer-to-Peer Electronic Cash System", and it laid out a vision for a distributed digital money system.

In January 2009, Satoshi Nakamoto released the first version of the open-source bitcoin core software on SourceForge and the bitcoin protocol started running. Nakamoto mined the first 50 bitcoins. The protocol was a breakthrough in cryptography, though it drew on developments that had preceded it but hadn't been combined yet.Bitcoin ran quietly in the background—a topic of excitement and fascination for a dedicated crowd of coders but largely off the world's radar. Discussion was distributed across different forums, and it wasn't until the end of the year that the first dedicated forum was established. This helped coders could more easily coordinate with other coders as the underlying code got tweaked. By mid-2009, people other than Satoshi Nakamoto were actively contributing to the open-source codebase in Github.The protocol was a breakthrough in cryptography, though it drew on many cryptography innovations that preceded it. A community of cryptography experts and privacy advocates known as the Cypherpunks (cypher not cyber) played a key role in recognizing the technical genius of Bitcoin and understanding its implications. Many members of this community would become torchbearers later in Bitcoin's history.As 2009 ended, Bitcoin did not have a 'trade price' and 309 people viewed the Wikipedia page.

2010: BITCOIN'S VERY EARLY YEARS

The Bitcoin 'ecosystem' was largely just a record of Bitcoin transactions (the blockchain), a set of online forums where users communicated and organized transactions, and the open-source software code. There were no wallet services, payment processors, or real user interface beyond actual command prompts and raw code. This limited involvement to a dedicated and savvy crowd who organized transactions through online forums and

initiated them on the blockchain with code. For example, the first commercial transaction took place in May 2010: a programmer in Florida spent 10,000 BTC on a pizza.However, beginnings of a market support system began to emerge. In early 2010, the first exchange opened, which allowed structured trading of bitcoins. The first "article" on bitcoin appeared on Slashdot and stoked interest beyond the initial insider cryptocurrency crowd. Users grew. In late 2010, Mt. Gox launched as the second exchange and became the dominant place to trade Bitcoins for a couple years.As 2010 ended, the price of 1 Bitcoin was $.3 and 309 people viewed the Wikipedia page.

2011: Bitcoin finds niche uses and awareness grows

In 2011, Bitcoin began to mature as a digital payment system, though its use was limited by the aspirations of early adopters.The perceived anonymous nature of the digital currency made it perfect for online black markets. That year saw the emergence of the Silk Road, an ebay for illicit goods (predominantly drugs) that used Bitcoin as a payment method. The Silk Road was one of the public's primary introductions to Bitcoin, prompting several politicians cast the currency as a vehicle for money laundering and drugs.Mainstream media also began covering it. Forbes, Bloomberg, and TIME all wrote articles. Politicians warned against it. Academics wrote about it. At the end of the year, CBS aired an episode of the "The Good Wife" that focused on bitcoin.Other consumer services were also starting to emerge. WikiLeaks started accepting Bitcoin donations. An iPad app was launched. Bitpay, a service that let merchants accept bitcoins over the phone, was founded and claimed to have 100 merchants. More exchanges opened, letting people trade bitcoins for other currencies.The Bitcoin code also underwent a major change. Through 2011, Satoshi Nakamoto had overseen the maintenance of the codebase. Satoshi never called or met anyone and only communicated on forums and direct messages. In April 2011, Satoshi Nakamoto wrote his last verified email, leaving Gavin Andreson in charge of the project, and left, never to be (verifiably) seen or heard from again. Andreson quickly selected four others to share this responsibility and introduced some structured ways of updating the underlying code.Also in 2011, the first alternative digital currency or "altcoin", Litecoin, launched.The world was in an awkward time in which financial markets were doing well but workers were not. Occupy Wall Street started in September and soon Occupy protests had taken place in almost 1000 cities worldwide. It is easy to see how the idea of a bankless currency could take root.As 2011 ended, the price of 1 Bitcoin was $4.60 and 2185 people viewed the Wikipedia page.

2012: Bitcoin matures

Bitcoin was riding a wave of legitimacy in many circles, and these were having conflicting effects.The currency became a popular target for hackers and thieves. Mt. Gox had been hacked in 2011, and now more major attacks on exchanges and other databases led to millions of dollars worth of Bitcoin theft. Several Ponzi schemes ended with theft.Black markets utilizing bitcoin as a payment method continued to operate. It's estimated that $15 million worth of Bitcoin passed through the Silk Road this year. A popular online gambling site, Satoshi Dice, launched and flooded the bitcoin network with very small gambling transactions (bets worth less than $.0001). This sparked a debate on how to deal with such 'transaction dust.'More generally, the community was feeling the impacts of having no central authority. There were no dedicated funds to support core development of the code and no sanctioned gathering places places other than online forums.The Bitcoin Foundation was also

established. Its role was to fund core development, represent the currency to governments, and conduct outreach and education. Late that year, a Bitcoin exchange Bitcoin-central.net was licensed similar to a bank in Europe.As it garnered the attention of more governments, its legal ambiguity became more obvious and more awkward. People were trading it like an asset, using it like a currency, and downloading it like open-source software. Gambling and the Silk Road didn't help. Some services started dropping bitcoin out of fear of its legality.Broadly, this is a year in which the industry also saw the promise of banking the unbanked with Bitcoin. Forbes runs one of the first mainstream articles discussing Bitcoin's use in remittance payments. WordPress started accepting Bitcoin, explaining that traditional payment processor restrictions were preventing international bloggers from participating in the blogosphere.As 2012 ended, the price of 1 Bitcoin was $13.44 and 2809 people viewed the Wikipedia page.

2013: The world wakes up to bitcoin

2013 was one of the most tumultuous years for Bitcoin. It had two period of incredible volatility in which people literally woke up to almost 100% price increases.The first occurred in early 2013. A bail-out deal between the EU and Cyprus included a levy on bank accounts with sizeable sums of money, inspiring Cypriot account holders to buy bitcoin en masse. The Bitcoin price almost doubles, and Cypress sets a precedent for using Bitcoin as a means of capital flight.Bitcoin survived one of its first major crises of legitimacy this year: the shutting down of the Silk Road and the arrest of its founder. The government seized all assets and helped cement public association of Bitcoin with online black markets. After a quick price drop, the price quickly recovered, but Bitcoin has lived in the Silk Road's shadow ever since.Globally, governments began to take Bitcoin more seriously but reactions were mixed.

- The People's Bank of China, after initially approving Bitcoin, banned financial institutions from using it or working with customers whose businesses involve it.
- The US Department of Homeland Security declared Mt. Gox a 'money transmitter' (a heavily regulated entity) and moved to seize some of its assets.
- US Financial Crimes Enforcement Network (FINCEN) issued some of the world's first bitcoin regulation in the form of a guidance report for persons administering, exchanging or using virtual currency. In particular, exchanges must comply with money laundering laws and register as Money Services Businesses.
- The US Senate held a hearing which was (to the surprise of many) open to the long-term prospects of Bitcoin.

2014: Bitcoin beyond cryptocurrencies and cryptocurrencies beyond Bitcoin

In early 2014, Bitcoin survived another major crisis of legitimacy: the closure of Mt. Gox. Mt. Gox had been the longest-running and most successful virtual currency exchange to date. It was a pillar of both the bitcoin economy and the community. In February, Mt. Gox abruptly shut trading, and leaked documents show it had lost 744,000 BTC (approximately $40 million). Bitcoin naysayers had a field day on forums, and it was widely seen as a blow to the digital currency's ability to operate safely without any oversight or regulation.Governments began to pass regulation this year. The wild end to 2013 woke many regulators up to the volatility of this currency. The IRS declared Bitcoin to be taxed as property. The People's Bank of China forced Chinese banks to close the bank accounts of major Chinese exchanges, though many exchanges exploited

legal loopholes to keep operating. New York announced its Bitlicense: a legal licensing framework for businesses that interact with Bitcoin and cryptocurrencies. This is largely decried by the cryptocurrency community. The dream of unregulated cash was quickly fading.The currency also traveled more into the payment mainstream, and a wave of major retailers accepted the currency. Overstock, Tiger Direct, Newegg, Dell, and Microsoft all announced acceptance of Bitcoin. Near the end of the year, a subsidiary of PayPal announced it will work on integrating Bitcoin on their platform.\Another development in the world of cryptocurrencies is that many many people began imagining Bitcoin without the digital currency part: how could the underlying technology be used for other purposes? A wave of new protocols emerged with applications beyond digital currency, presaging a so-called "Bitcoin 2.0" era in which people would repurpose blockchains (Bitcoin's and others) to store all kinds of information.

2015: The business blockchain

The basic features of this industry mostly continued. Hacks and theft continued, including a high-profile loss of close to $5 million from a major exchange at the beginning of the year.Regulators around the world continued to explore the implications of this technology while also proving that users of Bitcoin are not beyond the reach of the law. Ross Ulbricht, founder of The Silk Road, is sentenced to life in prison without parole for actions that were "terribly destructive to our social fabric." Mark Karpeles, CEO of Mt. Gox, is arrested in Japan. Two federal agents who stole Bitcoin during the Silk Road investigation plead guilty.The biggest shift came from banks and industry. Many industry executives began talking about "blockchains" and "distributed ledgers" rather than Bitcoin. Microsoft launched blockchain-as-a-service (BaaS) on its Azure cloud-computing platform. This allows companies to experiment with blockchains and explore how they could be used in different areas of their business.This likely contributed to the growth in interest in Bitcoin among the broader public and among traders. Bitcoin's price began a steady ascent as people started realizing Bitcoin and blockchains were still around.However, a crisis was brewing in the form of the "block size debate." The Bitcoin protocol was designed to process approximately 7 transactions per second; the blocks in the blockchain were not large enough to store more. Members of the community realized Bitcoin was on pace to reach that in 2015. If nothing was done, it could stymie the currency's growth in popularity.What followed was a bitter and divisive debate about whether to increase the size of the Bitcoin blocks (allowing more transactions per second) or to reposition the Bitcoin blockchain as a 'settlement layer' while allowing other services to process transactions that happen off-chain. In Bitcoin, there are no democratic rules, public sanctioned spaces to gather, or Robert's rules of order. Reddit, Bitcointalk, and a couple other online forums were serving as venues for 'public' discussion, and the Bitcoin Foundation began hosting events toward the end of the year.No one could agree, and the debate was fierce. This deadlock struck a blow to Bitcoin's perceived legitimacy. If it couldn't deal with a challenge like this, how could it deal with others? People started talking seriously about other currencies that might be viable alternatives to Bitcoin. Ethereum topped that list, and in early 2016, its price would increase tenfold.As 2015 ended, the price of 1 Bitcoin was $426 and 4730 people viewed the Wikipedia page.

2016: A Year of Promise

It is too early to tell the story of 2016 for Bitcoin. Many of the trends that coalesced in 2015 continued: more enterprise and corporate interest in blockchain technology, more uncertainty over the block size debate, and

some price volatility.Security remains an issue. Just this year, Gatecoin, a major exchange based in Hong Kong, lost $2 million and suspended trading. Shapeshift, a major US-based exchange, suffered a series of hacks in a saga that reads like a crime novel.Broadly, industry players in finance and technology remain bullish on blockchains and ambivalent about Bitcoin. More and more startups are branding themselves as blockchain companies rather than bitcoin companies. A new ambivalence about Bitcoin has emerged: not as a dangerous quasi-legal currency but as a good proof-of-concept that ultimately won't be ready for primetime. As they say, "the pioneers get the arrows, the settlers get the land." At a premier industry conference, some compared Bitcoin to Netscape. But Bitcoin's price continues to rise.

V. 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 bitcoins 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, on your smartphone, on your tablet, or somewhere in the cloud.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.

VI. HOW BITCOINS ARE MADE??

A bitcoin, at its core, is a very simple data ledger file called a 'blockchain'. A blockchain's file size is quite small, similar to the size of a long text message on your smartphone.Each bitcoin blockchain has three parts, two of which are very simple: its *identifying address* (of approximately 34 characters), and the *history* of who has bought and sold it (the ledger).The complex part of the bitcoin is its third part: *the private key header log*. This header is where a sophisticated digital signature is captured to confirm each and every transaction for that particular bitcoin file.Each digital signature is unique to each individual user and his/her personal bitcoin wallet. These signature keys are the security system of bitcoins: Every single trade of bitcoin blockchains is tracked and tagged and publicly disclosed, with each participant's digital signature attached to the bitcoin blockchain as a 'confirmation'. These digital signatures, when given several seconds to confirm their transactions across the network, prevent transactions from being duplicated and people from forging bitcoins.Note: While every bitcoin records the digital address of every bitcoin 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.Your bitcoins are stored on a computer device of your choice, but the history of each bitcoin you own or spend is publicly stored on the bitcoin network, and every user will be able to see every bitcoin's history.While people cannot easily see your personal identity, people 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.You can see bitcoin transactions

at blockchain.info. These are public ledgers of all the bitcoin wallets on the planet. Note: There are no people's names attached; the wallets themselves are completely anonymous.

VII. 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.

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.

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 themselves.

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 is 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, then your wallet's contents are gone forever.

VIII ADVANTAGES

- People no longer have to rely upon the bankers who have been handling their money for generations to make a transaction. So transferring funds becomes easy.

- Fundamentally changes the financial services industry – by dropping the cost and complexity of financial transactions, making the world's unbanked a viable new market.
- Bitcoins could reduce banks' infrastructure costs by15 – 20 billion dollars per annum by 2022.
- Bitcoin transactions cannot be reversed, do not carry with them personal information, and are secure, merchants are protected from potential losses that might occur from fraud.
- The Bitcoin software is completely open source and anybody can review the code.
- Transaction cost is very little, especially compared to other payment networks.
- Bitcoin is changing finance the same way the web changed publishing.
- Bitcoin being a digital code is infinitely more durable than paper currency, unless someone shuts down the entire internet.
- Since bitcoins are created by crypto-currency mathematical algorithm, they are much harder to counterfeit than paper currency.

IX. DISADVANTAGES

- Lack of Awareness & Understanding.
- It undermines the authority of banks and financial institutions on the financial system.
- Bitcoin prevents any government and financial institution from acting as a trusted third party to facilitate transactions.
- There is still no legal framework protecting the rights of users of these technologies or overseeing the institutions that use them.
- Bitcoin has volatility mainly due to limited amount of coins and the demand for them increases day by day.
- Bitcoins have been banned in several countries on grounds that these currencies could be used for money laundering, terror funding and drug trafficking.
- It's very much still an experimental currency and is a high-risk environment for consumers and investors at the moment.
- Problems such as losses arising out of hacking, no sources of customer recourse and the general financial volatility surrounding Bitcoins.

X. CONCLUSION

Since the establishment of Bitcoin 2009, its uses as a cryptocurrency have been debated extensively as it has become a highly controversial topic. The debates are stimulated by the fact that some argue it has the potential to disrupt the financial system as we know it. On a positive note, the minimal fees and lack of regulations makes it much easier and cheaper to send money internationally. This ultimately makes capital available in the places that need it the most and were previously unable to gain access to capital flows. However, when looking at the negatives, the implementation of this currency also allows for the facilitation of criminal activity, and it takes away from the ability of the government to generate revenue through taxation. This tradeoff highlights the importance of cost-benefit analysis when evaluating the issue. Furthermore, it is critical to note that any

(ICRIME-17)
ISBN: 978-93-86171-50-4

alterations made to the existing infrastructure could radically change the nature of the currency and eliminate some of the greatest benefits it was designed to retain.

REFERENCES

1. https://en.wikipedia.org/wiki/Bitcoin
2. https://www.coindesk.com/information/what-is-bitcoin/
3. https://bitcoin.org/bitcoin.pdf
4. https://en.wikipedia.org/wiki/History_of_bitcoin
5. http://www.newsbtc.com/2015/03/23/bitcoin-mining-start/
6. https://bitcoin.org/en/how-it-works
7. https://www.smithandcrown.com/a-history-of-bitcoin/