# ON CRYPTOCURRENCIES: AN ASSESSMENT OF BITCOIN'S PROSPECT AS LEGAL MEDIUM OF EXCHANGE

**Kazi Md. Nasir Uddin**[*]

## Abstract

*Digital currency or virtual currency has gained importance in recent times. But various complexities associated with its definition, made this currency ambiguous to society and financial institutes alike. Digital currencies are used in real-world transaction as well as in the dark web. The currency comes into discussion with the creation of bitcoin, which is an online payment method taking place between users directly through a peer-to-peer system without any intermediary or financial institute. Although the payment process requires digital signature, a third party is needed to prevent double spending in the transaction, which can be done by a peer-to-peer network. Online bitcoin payment system is invented and used through an open-source code. Its security and secrecy are protected cryptographically and transactions are conducted and preserved in an organized way. As a result, the number of bitcoin account holders has been increasing considerably. We can use bitcoins legally besides other legal tenders, if existing laws do not consider these coins immoral. Also, in the midst of the ongoing global pandemic (Novel Coronavirus or Covid-19), a paperless currency like bitcoin, which also involves contactless transaction, would go a long way in preserving wellbeing for individual and economy alike. Furthermore, we can try to find out and address the problems related to this currency. After proper assessment, if we acknowledge bitcoin, they can compete with the existing coins in the present currency system, complying with government rules, and contribute to the development of the currency system. They can also work as service providers or economic agents of virtual coins, and participate in the country's economic activities through the exchange of the coins.*

***JEL Classification*:** E42; G18; O38

***Keywords*:** Cryptocurrencies; bitcoin; Digital currencies; Virtual currencies; Cryptography; Fiat currency; Covid-19

[*] Associate Professor, Department of Accounting & Information Systems, Jagannath University, Dhaka, Bangladesh.

***“Virtual currencies, perhaps most notably Bitcoin, have captured the imagination of some, struck fear among others, and confused the heck out of the rest of us.”*** – Thomas Carper, US-Senator.

## 1. Introduction:

Money forms the backbone of the modern economy as without money modern economies cannot function (Asmundson and Ceyda, 2012). Mishkin (2007) stated that money is any bits and pieces or provable record that is generally accepted as payment for goods or services and reimbursement of liability in a particular country or socio-economic context. Thus, money includes coins, currency notes, cheques, bills of exchange, and so on. The Wall Street psychologist dot com (2015) mentioned that money is basically described as fiat money like any check or debt that excepting use value as a materialistic commodity. Thus, it has legality that money must be accepted as a form of exchangeable payment within the territory of the country for all financial transactions’: public and private alike.

In contemporary era, money took an electronic form namely, crypto currency. During this ongoing global pandemic[2], when worldwide economic growth has been stalled, trading with bitcoins registered a record high on 17 November, 2020. On that day, trading figure of bitcoins registered above USD 17,000, and an increasing number of stakeholders sponsored it as an alternative to other currency or gold or assets. According to financial analysts, the pandemic had the stakeholders rejuvenated to assess a long-term outlook for bitcoin and other cryptocurrencies such as Ethereum, Litecoin and XRP.

How can the word “Cryptocurrency” be defined and how can it be clarified? Is it virtual, transferable, secret or hidden, electronic currency of the future? How it is designated and recognized by government, and central banks? Would this currency play a dominant role in digital transaction? All major financial institution prefer the phrase “virtual currency”- recognized that cryptocurrency as digital currency and recognized it as a parallel world of the computer network.

The current paper tries address these questions. The paper also reviews the antecedents of Cryptocurrencies. The protocol, controlling and regulatory aspects are focused and touched leading in the section on propositions. Major part of discussion is encircled around bitcoin. The existing versions of cryptocurrency or virtual currency are paying attention on copycats, regulatory irregularities and governments’ barriers or constraints. A body of literature, academic and supplementary, are reviewed on the technical knowhow of cryptocurrency. Antonopoulos (2014); Franco (2015); Swanson (2014) are the most important sources for understanding bitcoin. However, financial perspective is not only the main focus of their study but also, they focused on

[2] https://www.theguardian.com/technology/2020/nov/17/bitcoin-jumps-to-three-year-high-as-covid-crisis-changes-investor-outlook

paperless transactional society. Cryptocurrencies are not instantly sufficient on the basis of financial view.

## 2. The history of Cryptocurrencies

Technical foundations of Cryptocurrency's date back to the early 1980s when Chaum attempted to introduce another concept of commercialize blinded money or cryptocurrency. In Netherlands, Chaum established DigiCash based on the blinding algorithm. Chum, Fiat, & Naor (1990) described that first time for using the encrypted keys for withdrawing money from a bank was untraceable by the issuing bank, government or third party.

Laurie, Sabett and Solinas (April, 1997) have explained in details. Afterwards, Chaum, Szabo and Nick (December, 2005) introduced a cryptocurrency namely "bitgold" (gold-based exchange transaction unit), which was important to use the system of blockchain that foot marked the modern cryptocurrencies.

The end of DigiCash, opened room for further research and investment in electronic financial transactions by modifying more conventional, though digital mediator such as PayPal and others. The DigiCash copycats; such as Russia's WebMoney (cryptocurrency) sprang up in other parts of the world. At the mid-2000's e-gold had millions of active accounts and processed billions of dollars in transactions annually.

Nakamoto (2008) conceptualized the decentralized cryptocurrency and introduced the first decentralized cryptocurrency "bitcoin" that is now widely considered the peer-to- peer electronic cash system. In late 2012, for the first time WordPress**,** Expedia, and Microsoft started to trade by accepting payment in bitcoin . On screen, cryptocurrency as a legitimate payment method was used by dozens of merchants. The UK News (2014) published an article on "UK launches initiative to explore potential of virtual currencies" where Chancellor George Osborne told UK Treasury to conduct a study on cryptocurrencies, and its possible role in the UK economy.

## 3. Cryptocurrency[3]

Cryptocurrencies are maintained by cryptographic protocols, which is written on advanced mathematical logic and computer engineering principles that make them virtually impossible to crack, and duplicate or fake protected. Also, the identities of cryptocurrency users disguise by protocols, transactions and fund flows ensures its safety.

[3] https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives- "What Is Cryptocurrency – How It Works, History & Bitcoin Alternatives" By Brian Mariucci

### 3.1.1. Decentralized Control

The controlling systems of Cryptocurrencies are ensured by decentralized control. Cryptocurrencies are not directed by government or other regulatory bodies. it is simply directed by its users and protocols built into their governing codes.

### 3.1.2. By exchanging Cryptocurrencies with Fiat Currencies

With due consideration to emphasize, cryptocurrencies with fiat currencies can be converted for transaction in special online markets, that means every moments cryptocurrencies would carry the variable exchange rate with major world currencies like U.S. Dollar, British Pound, Euro , and Japanese Yen.

### 3.1.3. Supply limitation

By predetermined supply, the majority but not all, cryptocurrencies are differentiated. It will become difficult for minors to produce the units of those currencies, until the upper limit is reached and ceases to new currency to be minted. Cryptocurrencies source codes contain commands demarcation the precise number of units that can and will still be real. Innately deflationary for cryptocurrencies' fixed delivery, more similar to gold and supplementary precious metals of which there are limited supplies than fiat currencies.

### 3.1.4. Advantages and Limitations

Users of cryptocurrencies are not located by the government. So, one kind of freedom would be enjoyed by the owners compared to the fiat currency users. Government intend to cease the fiat currencies from legal or illegal citizens but it is not possible to do that due to nature of cryptocurrencies that means political sovereignty and basically impassable data security ensured in cryptocurrency than conventional fiat currencies.

On the contrary, some risks are associated with cryptocurrencies as they are difficult to convert to cash. In addition, commonly gray and black-market transactions are used to make easy by cryptocurrencies. And while cryptocurrencies open up an alternative avenue for lucrative investments, they are mostly subject to pure speculation.

## 3.2. Working systems

Cryptocurrencies are highly protected due to its logic-based source codes and scientific controls that ensured the security and support. Though, general public are more than capable of properly understanding the concepts and appropriate knowledgeable cryptocurrency users. Meaningfully, most cryptocurrencies are differences on bitcoin.

### 3.2.1. Wei dai protocol

In the first protocol[4], all accounts mutually define the ownership of money, and how these accounts are operated.

1. The creation of money

Anyone can create money by broadcasting the solution to a previously unsolved computational problem given that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual. The number of monetary units created is equal to the cost of the computing effort in terms of a standard basket of commodities.

2. The transfer of money

If someone wishes to transfer a certain amount of money to another person, the sender would broadcast a message and the system would debit the sender's account and credit the receiver's account by the mentioned amount in the message.

3. The implementation of contracts

A valid contract must include maximum reparation in case of default for each participant party and include a party who will perform arbitration should there be a dispute. All parties to a contract including the arbitrator must broadcast. Their signatures of it before it becomes effective and accordingly, every participant debits the account of each party by the amount of his maximum reparation and credits a special account identified by a secure hash of the contract by the sum the maximum reparations. Otherwise the contract is ignored and the accounts are rolled back.

4. The conclusion of contracts

If a contract concludes without dispute, each party broadcasts a signed message and every participant credits the account of each party by the amount of his maximum reparation, removes the contract account, then credits or debits the account of each party according to the reparation schedule if there is one.

5. The enforcement of contracts

If the parties to a contract cannot agree on an appropriate conclusion even with the help of the arbitrator, each party broadcasts a suggested reparation/fine schedule and any arguments or evidence in his favor and makes a determination as to the actual reparations and/or fines and modifies his accounts accordingly.

[4] http://www.weidai.com/bmoney.txt

In the second protocol[5], the accounts of who has how much money are kept by a subset of the participants (called servers from now on) instead of everyone. These servers are linked by a use net-style broadcast channel. The participants of each transaction should verify that the message has been received and successfully processed by a randomly selected subset of the servers.

So, I propose an alternative money creation sub-protocol, in which account keepers (everyone in the first protocol or the servers in the second protocol) instead decide and agree on the amount of b-money to be created each period, with the cost of creating that money determined by an auction which is divided up into four phases:

#### 1. Planning

The account keepers compute and negotiate with each other to determine an optimal increase in the money supply for the next period and if the account keepers can reach a consensus, they each broadcast their money creation quota and any macroeconomic calculations done to support the figures.

#### 2. Bidding

Anyone who wants to create b-money broadcasts a bid, then form <x, y> where x is the amount of b-money he wants to create, and is an unsolved problem from a predetermined problem class and each includes a nominal cost (in MIPS-years say) which is publicly agreed on.

#### 3. Computation

After viewing the bids, the ones who placed bids in the bidding phase may now solve the problems in their bids and broadcast the solutions.

#### 4. Money creation

Each account keeper accepts the highest bids (among those who actually broadcasted solutions) in terms of nominal cost per unit of b-money created and credits the bidders' accounts accordingly.

### 3.2.2. Blockchain

Blockchain works as a master lager which records and stores all prior transaction and activity of cryptocurrencies as well as authenticating ownership of all units of the currency at any specified point in time. Like the record of a cryptocurrency’s whole transaction history to date, a blockchain has a fixed length – containing a fixed number of transactions – that enhanced over time to time. Blockchain alike copies are stored in every node of the cryptocurrency’s software network which stored decentralized server, control and run by computer analyst individuals or groups of individuals who introduced as miners who repeatedly record and validate cryptocurrency

[5] http://www.weidai.com/bmoney.txt

transactions. Every transaction of cryptocurrencies is not finalized until those transactions add in to the blockchain, which generally takes within minutes. Every transaction is irreparable when the time it’s finalized. Double-spending, or manipulation of cryptocurrencies prevent by blockchain, also restricted same currency duplication and many receivers.

### 3.2.3. Private Keys

Every cryptocurrency account holder publishes his or her account identity by a private key which is generated from systems that key contain 1 to 78 digits to formulate randomly by the systems, this private not only authenticated account holder identity but also permit to get ownership and exchange of cryptocurrencies units. When account holder gets the key, they have the right to obtain or spend or convert the cryptocurrencies. Without getting that private key, the worth on cryptocurrencies would be zero. The security features of this private key restrict unlawful use and reduce robbery. If one looses the private key and can easily create another key again. So, cryptocurrency account holder preserves their private key in analog location or stored in internet less storing house.

### 3.2.4. Wallets

Every Cryptocurrency user automatically have “wallets” which contain identical information to confirm the temporary ownership of their cryptocurrency’s units back to back private key has confirmed the transaction authenticity of cryptocurrency. Wallet made sure to reduce risk to theft unused cryptocurrencies which stored in that wallet.

Wallets stored on the cloud, an internal hard drive, or an external storage device. At least one backup is strongly proposed for safety of main wallet.

### 3.2.5. Miners

Miners as record-keepers are for cryptocurrency societies and indirect authorities of the cryptocurrincies’ value. Miners use highly protected technical systems or methods to authenticate the completeness, exactness and safety of currencies block chain.

Miners’ work is to make new copies of the block chain periodically. Now adding, any earlier unverified transactions could not include in any prior block chain copy without completing those transactions effectively. Blocks consist of all transactions which executed earlier in new copy of the block chain was created.

### 3.2.6. Predetermined Supply

Nature of fiat currencies is unlimited supply, but cryptocurrencies supply is limited like precious metal (gold). Though mining creates cryptocurrency units (new) periodically, but all-time cryptocurrencies are calculated to have a limited supply. Here basic concepts about cryptocurrencies are that miners receive or create fewer currency units (new) per block chain (new) after sometimes. Miners would receive transaction fees for their work finally.

### 3.2.7. Cryptocurrency Exchanges

Cryptocurrencies exchange system that means crypto to fiat or liquid and liquid to crypto is not very easy. They can only be exchanged through private currency house, peer-to-peer transfers. Popular cryptocurrencies, such as bitcoin and Ripple, trade on special secondary exchanges markets like forex exchanges for fiat currencies (Mt. Gox is one example) like above stated secondary exchange markets allow cryptocurrencies account holder to exchange their cryptocurrency worth for major fiat currencies, such as the USD and Euro, and other cryptocurrencies (including less-popular currencies).  Those exchangers would be charged very little for each transaction which is less than 1% of those transactions.

Now in present situation, exchange pricing can still be unpredictable, which triggered bitcoin's - USD exchange rate to collapse by more than 50% in the wake of Mt. Gox's collapse, then enlarged roughly ten times during 2017 as cryptocurrency stipulated. bitcoin is the top cryptocurrency and first to be used popularly and widely. Though, hundreds of cryptocurrencies running in the market and newly spring into being every month.

## 4. bitcoin

Nakamoto (2008) outlined a payment system that addressed the double spending problem of digital currencies**.** Many have speculated that he is not just one person but rather a collective pseudonym for a group of cryptographic developers. Some have come forward claiming to be Satoshi, but to date; his real identity remains a secret. The concept on bitcoin had been published after some days; the bitcoin project software was registered in Source Forge. bitcoin block called the 'Genesis block' was mined the first time ever in January 2009. Days after, the first ever bitcoin transactions have seen in the virtual world- block 170 recorded transaction between Hal Finney and Satoshi Nakamoto.

Franco (2015) wrote that the bitcoin is created by cryptographically coded systems to ensure the high security. The prefix "Crypto"- is attaining a well-defined meaning. The currency unit names are bitcoin (BTC), milibitcoin (mBTC=$10^{-3}$), microbitcoin (µBTC=$10^{-6}$) and satoshi ($10^{-8}$).

The currency "bitcoin" is depended and directed by payment dealing out work for transactions. Transaction is recorded by user provides computing power, and payment is maintained in a public ledger thereof. This methodical system or process is called mining. All transactions of bitcoin completed after the verification. Afterwards share the ledger in publicly then it is recognized or useable for payments. Transactions of this bitcoin are combined into blocks approximately every ten minutes. The legitimacy of transactions of bitcoins has proved by block which requires vast computation power but verifying need little computation power. If mining is done competitively on the network, transactions are confirmed transparently to ensure by creating trust. The new bitcoin for each block creates by mining process. The quantity of bitcoin for per block is predetermined and reduces with time. In 2009, fifty  bitcoin per block was first started the process and the rewarded halves after 210,000 blocks. In 2040, when all bitcoins are about 2,10,00000 then may all mining process may be stopped which concept established by mathematically on basis of bitcoins systems.

W. Mougayar (2014) stated the 8 identities of Bitcoin which roughly consists in present functioning system of bitcoins followed as (1) A virtual currency which built in cryptography coding to ensure the security of bitcoins. (2) Peer-to-peer cash systems which functioning without any third parties. (3) The concept is directed and implemented by solitude and secrecy force behind the screen in the network systems. (4) Open-sources networked provided and derived by a volunteer group of developers those are openly controlled mining and transaction of bitcoins. (5) By encrypting and bookkeeping (blockchain) to use non-centralized computing network. (6) Fixed money creation which limiting the manipulation of bitcoins currency without screening government rules and regulations. (7) Free to define the boundaries and regulate the use of the “bitcoins” from National authorities. (8) A virtual currency with fluctuating exchange rates for major currencies of the world.

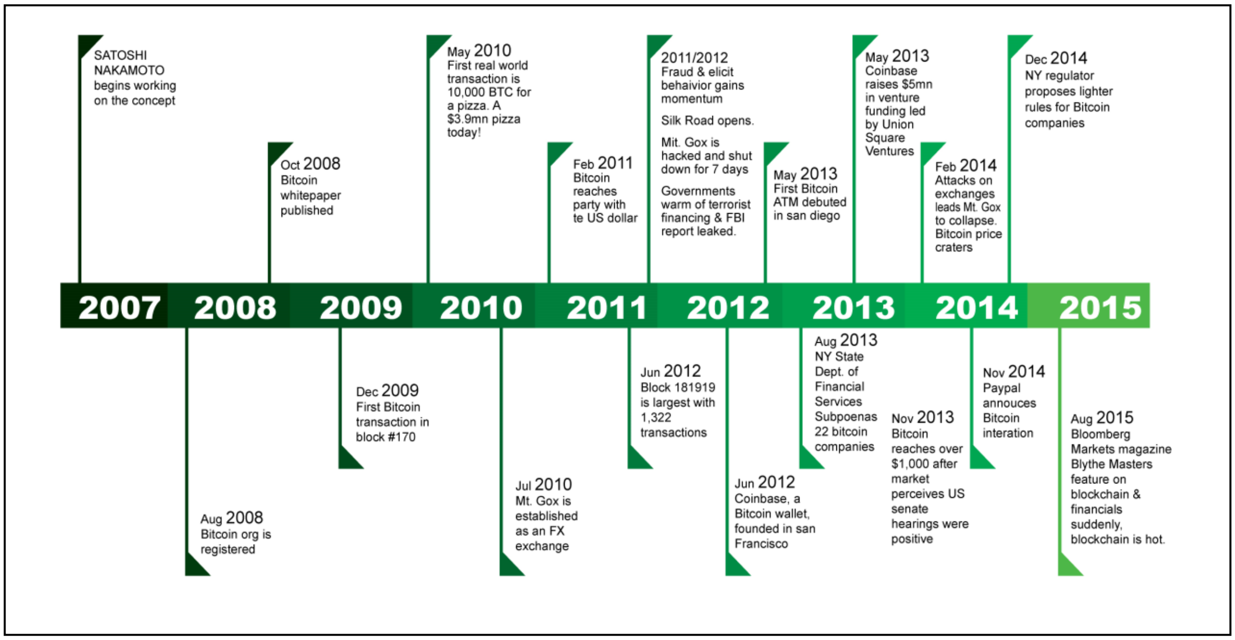
Above stated identities are listed in the following table:

| | Description | Quantity |
|---|---|---|
| I. | BTC Economy | |
| 1 | Total BTC | BTC 16,522,800 |
| 2 | Market capitalization | USD 146,403,573,960 |
| | | EUR 120,533,826,000 |
| | | GBP 104,645,171,064 |
| 3 | Transactions (last 24 hours) | 2,46,531 |
| | Transactions (average per hour) | 10271 |
| 4 | BTC sent (last 24 hours) | 1761138 BTC |
| | BTC sent (average per hour) | 73381 BTC |
| II. | Blocks | |
| 1 | Count | 481,823 |
| 2 | Blocks (last 24 hours) | 149 |
| | Blocks (average per hour) | 6 |
| 3 | Difficulty level | 923,233,068,449 |
| | Next difficulty level (in 1831 blocks) | 887,736,944,047 |
| 4 | Network hash rate (terahashs per second) | 6354668.57 |
| | Network hash rate (petaFLOPS) | 80704290.84 |
| III. | Nodes | |
| | Reachable nodes | 10536 |
| IV. | Transactions | |
| | Transactions (since inception) | 312252902 |
| V. | Accounts | |
| | Accounts (since inception) | 24,343134 |
| VI. | Blockchain Size | |
| | Size | 165175 MB |
| VII. | Businesses | |
| | Number accepting BTC | >100,000 |
| VIII. | Mining Cost | |
| | Total miners revenue (last 24 hours) | USD 18085957.93 |
| | % earned from transaction fees (last 24 hours) | 3.61 |
| | % of transaction volume (last 24 hours) | 1.08 |
| | Cost per transaction (last 24 hours) | USD 71.33 |

Sources: I and II http://bitcoincharts.com/bitcoin/. III. https://getaddr.bitnodes.io/.IV.https://blockchain.info/charts/n-transactions total?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=.V. https://blockchain.info/charts/my-wallet-n-users. VI. https://blockchain.info/charts/blocks-size. VII. http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613. VIII. https://bitinfochart.com/bitcoins, as of April 25, 2018.

### The development schedule[6] of bitcoin as follows:

In 2007, Nakamoto (2008) begins work on the bitcoin concept. After that Aug 2008 Bitcoin.org domain was founded  and on October 2008 Bitcoin white paper was introduced. Most important facts in 2009 are the release of bitcoin version of 0.1 and the first transaction of the bitcoin currency and BTC exchange rate USD 1= 1,309.03 BTC.


SATOSHI NAKAMOTO begins working on the concept
Oct 2008 Bitcoin whitepaper published
May 2010 First real world transaction is 10,000 BTC for a pizza. A $3.9mn pizza today!
Feb 2011 Bitcoin reaches party with te US dollar
2011/2012 Fraud & elicit behaivior gains momentum
Silk Road opens.
Mit. Gox is hacked and shut down for 7 days
Governments warm of terrorist financing & FBI report leaked.
May 2013 First Bitcoin ATM debuted in san diego
May 2013 Coinbase raises $5mn in venture funding led by Union Square Ventures
Feb 2014 Attacks on exchanges leads Mt. Gox to collapse. Bitcoin price craters
Dec 2014 NY regulator proposes lighter rules for Bitcoin companies
2007
2008
2009
2010
2011
2012
2013
2014
2015
Aug 2008 Bitcoin org is registered
Dec 2009 First Bitcoin transaction in block #170
Jul 2010 Mt. Gox is established as an FX exchange
Jun 2012 Block 181919 is largest with 1,322 transactions
Jun 2012 Coinbase, a Bitcoin wallet, founded in san Francisco
Aug 2013 NY State Dept. of Financial Services Subpoenas 22 bitcoin companies
Nov 2013 Bitcoin reaches over $1,000 after market perceives US senate hearings were positive
Nov 2014 Paypal annouces Bitcoin interation
Aug 2015 Bloomberg Markets magazine Blythe Masters feature on blockchain & financials suddenly, blockchain is hot.

Pictorial History of Bitcoin (Source: Leemoon, 2017:5)

bitcoin's market ceiling went above USD 1,000,000 within November 2010. That was a key time for the development of bitcoin market as the investors invested capital in bitcoin. The price was USD 0.50/BTC in 2010 and reached USD 31.91/BTC which highest price within June 2011. That period was referred as "Great Bubble of 2011". Four days later, the exchange rate dropped to just USD 10/BTC[7].

## 5. The economics of bitcoin

Now, how bitcoin performs as money? Miller, Michalski and Stevens (2002) stated many points about function of currency or money and necessary attributes to success of digital currency. In future a lot of digital or non-digital currency will be created in point of digital or non-digital view and may be established digital or physical transaction systems. Some difficulties of digital currency express here:

[6] https://adioma.com/@depart/infographic/history-of-cryptocurrency

[7] https://successresources.com/cryptocurrency-history/- So what's the story behind Cryptocurrency?

“*there are some obstacles to realizing……peer-to-peer digital money that is network based, transparent, easy to use and highly secured. The difficulty most often raised when considering this [development] is the connection that network transaction will never be able to acquire the virtues of anonymity, accessibility and security that characterize hard cash….Gradually the same degree of difficulty that now accompanies the recording of serial number of hard cash as a way of tracing each transaction will arrive in the digital world, as cryptography, legal safeguards and protocols for erasing identity become widespread and efficient*.” (Page 18).

They forecast

“*Digital money will only match the attributes of physical cash if there are major advances in the ease, cost and certainty with which digital transaction are handled. In particular there will need to be considerable progress in the following areas: verification, confidentiality, ease of use, interoperability and reliability-throughout the entire transaction chain.*” (Page-19).

They are hopeful that

“*Eventually, with almost all of the current disadvantages of digital money out of the way, the vast share of consumer means of payment could tip over into the digital realm.*” (Page-19).

It is clear from these above statements that cryptocurrency like bitcoin performs the function of money.

**bitcoin as a medium of exchange**: Cuthbertson (2015) forecasted that 1,00,000 worldwide merchants likeOverstock.com, Virgin Galactic, Zynga, PayPal, Tesla Motors, OkCupid, The Pirate Bay have accepted BTC and rapidly increased the number. Earlier depicted table shows clearly how bitcoin serves as medium of exchange.

**bitcoin as a unit of account:** Unit of account holds a measure and a standard may be controversial but BTC performs as a unit of account. BTC is able to exchange with fiat currencies of 40 countries approximately. Koning (2013) stated that if the currency- prehistoric, medieval or contemporary is convenient then all big merchants of the world – are accustomed to their trading on that currency and function separated by medium-of-exchange function and unit-of-account function provides interesting lesson from medieval European history in his essay. One example is Arab Monetary Fund; it’s unique for its accounting system. The Dinar (Arab currency), its unit of account, is equivalent to three SDRs (Special Drawing Rights- created by IMF).

**bitcoin as a store of value:** From the ancient period, on the views of financial market situation any transaction made by exchange which ensured by any exchangeable recognized currency of on that time. Country or market demand or lack of money makes money and essentiality of exchangeable currency hold its value for a longer period. Both theatrically and actually bitcoins supply is predetermined and also limited. In spite of fluctuations of exchange rate, BTC certainly functions as a store of value.

**bitcoin and motives to hold a (cash) balance:** Andreessen (2014) quoted about bitcoin-

*"bitcoins gives us, for the first time, a way for one Internet user to transfer aunique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer*."

**bitcoin as a safe guard against crises:** During the 2008 global financial turmoil it was proposed in a released whitepaper that bitcoin had a role to play in this crisis period. Such role of bitcoin was again appraised by investors and stakeholders during the 2012-13. As cash and assets had become inaccessible, bitcoins draw much attention. Also, in Greece, amidst its deepest economic turmoil, the country laid down plan to adopt bitcoin as currency. Also, bitcoin offers an efficient way of to safeguard against highly contagious virus like Covid-19, as bitcoin trading is evidently paperless and contactless. Also, there were breakthroughs in policies and strategies related to cryptocurrencies. For example, "Digital assets or currencies" were the centre of discussion in the IMF's last annual meeting, where Fed Chairman Jerome Powell discussed bitcoin and America's potential plans for a national digital currency. Last December, Forbes had their first edition of "Cryptocurrency Awards", where Powell was named "Person of the Year in Crypto"[8]. All these suggest a growing role of bitcoin in crisis period.

**bitcoin is a key currency in the eras to come**: Prediction about bitcoin outlook is not easy, but evidence of its success during the pandemic period suggests a great deal of its potential. In 2020, bigger stakeholders like the US and EU showed interest in adopting bitcoin as it has technological benefits. They depicted their eager to have their own digital currency like China's digital Yuan. As such, governments across the world began launching new framework to control a central definition for the asset. A recent empirical work by financial researcher John O. McGinnis revealed that around 20% Australian adults own bitcoin. What makes bitcoin an attractive mode of transaction? It could be bitcoin's intangible and simple storage and incorruptible transactions, which make it a model currency to safeguard funds against the economic trials and variations that the future holds. Also, during this global pandemic, bitcoin has been accepted by governments worldwide as a new dimension of assets or currencies. Specially to counter the global economic crisis caused by Civid-19 shutdowns, bitcoin becomes one of the most valuable tools as it is capable to run numerical easing programs and adding liquidity to the system. Also, there is another dimension of bitcoin's role in perspective of Covid-19. As mentioned, bitcoin is paperless; hence transactions are free of any physical contact. It increases the appeal of bitcoin to stall the spread of any contagious diseases like Coronavirus.

[8] https://zerocap.oi/bitcoinforyourfuture/

To conclude it would not be an overstatement to state that BTC fulfils the function of currency sufficiently, though not completely. If the past decade indicates what the next few decades might look like, then we have firm evidence that bitcoin is here to stay.

## 6. Prospects, Challenges and barriers:

### 6.1. Prospects

By comparing the other currency with virtual currency like bitcoin is easy to exchange, and low transaction fees. Multiple ownerships are possible for the large transaction of bitcoin. bitcoin is alternative payment systems instead of *Hundi*. If one's have a computer with an internet connection and an account then it is very easy to access for transaction of bitcoins. Portability of bitcoins approximates like cash. Bitcoin is durable as any currency other than little exception. It is maintained highly secured functioning and transactional systems and are saved from forgery and counterfeiting. bitcoin systems are not possible to dominate by hostile governments. The divisibility of bitcoin which is acceptable in range, it is smallest sub-unit is shatoshi ($10^{-3}$). In bitcoin payment systems, any business organization can develop its own payment systems. Bitcoin is a deflationary currency. The bitcoin maintains software based on open-source so it adopts any innovation from any users or people. It is not possible to create any disputes with related parties. Now, with much protection, concerns about fraudulent exchange in cryptocurrencies which might led to loss of millions of dollars' worth of coins, seem to have declined, thereby giving stakeholders a greater security. "The virus crisis is propagating the reassessment of bitcoin," said Panigirtzoglou (2020), an analyst JP Morgan. "There is a reassessment about its value here as an alternative currency; as an alternative to gold."[9]

### 6.2. Challenges and barriers

Bitcoin is not legal tender and its raise doubt about its viability. In present situation bitcoin is an illegal currency in underdeveloped countries due to government and regulatory body could not be defined the currency and did not get the decision how to operate the currency. Bangladesh bank published a government notification to restrict the transaction of bitcoins. Bitcoins' transaction still carries on criminal risk for financial crime. Bitcoins' account holder forgets or lost their private key then they lost their currency. Bitcoin transaction is irreversible that means any transaction was made a mistake that is not correctional. Government is derived from revenue in the current transactional process of bitcoins. Transaction's verifying systems took time. An attack on cryptography of the currency could destroy not only bitcoins but all cryptocurrencies. It is out of the coverage of judiciary systems so any disputes happen with the related parties it could not be soluble in judiciary. Government trust is necessary to flourish bitcoins as like fiat currencies**.**

[9] https://www.theguardian.com/technology/2020/nov/17/bitcoin-jumps-to-three-year-high-as-covid-crisis-changes-investor-outlook

## 7. Concluding Remarks

Bitcoin is one of the leading Cryptocurrencies sparks the financial world and thus raises a lot of questions. Bitcoin network and other cryptocurrencies will draw an attention as disruptive innovation in the financial world. It is a very lucid concept for those one's who recognized on the contrary it is unruly idea. But everybody understood that bitcoin burst the concept which will be crate debate for long time. It is the finest decentralized idea in the financial currency transaction world which completes the transaction between two parties without interruption other parties which methodological, transparent and secured. Bitcoin is introduced the new arena where is not necessary paper-based currency but whole world is not prepare to accept it. In future bitcoin or other virtual cryptocurrency strike the currency market full throttle. In this regard, some recommendations are stated below:

1. Bitcoin's store of value for credit purposes needs to enhance.
2. Government needs to recognize it to minimize the risk of illegal transaction.
3. Credit system around bitcoin needs to be taken care of.
4. The liquidity of bitcoin needs to be improved.
5. Role of bitcoin in case of stability of asset prices needs to be clarified.
6. Role of bitcoin needs to be reassessed to counter any future crisis emerged from pandemic.

## References

[1] Andreessen, M. (2014, January 21). Why bitcoins matters. *New York Times*. Retrieved from http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?smid=pl-share

[2] Antonopoulos, A. M. (2014) *Mastering Bitcoin*. O'Reilly Media, Sebastopol.

[3] Asmundson, I., & Ceyda Oner. (2012) Back to Basics: What Is Money? *Finance & Development. International Monetary Fund,* Sept. 2012. Web. 14 Nov. 2015. Retrieved from http://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm>.

[4] Chum, D. et.al. (1990). Advances in Cryptology In Goldwasser (Ed.), *Untraceable Electronic Cash*, 319-327, Springer: Verlag, Berlin Heidelberg.

[5] Cuthbertson, A. (2015, February 4). Bitcoin now accepted by 100000 merchants worldwide. *International Business Times.* Retrieved from http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613.

[6] Dai, W. (1998). *B-money*, Retrieved from http://www.weidai.com/bmoney.txt.

[7] Franco, P. (2015). *Understanding bitcoin: Cryptography, engineering and economics.* Wiley, Chichester.

[8] Goldsborough, R., (2003, October 2). *World's first coin*. Retrieved from https://rg.ancients.info at 20th April 2009.

[9] Rosic, A., (n.d.). Retrieved from *https://blockgeeks.com/guides/what-is-cryptocurrency/*

[10] International Monetary Fund. (2015). *Fact sheet: special drawing rights (SDRs).* Washington DC: IMF. Retrieved from http://www.imf.org/external/np/exr/facts/sdr.htm

[11] Koning, J. P. (2013, September 13). *Separating the functions of money: The case of medieval coinage moneyness* (The Blog of J.P. Koning). Retrieved from http://jpkoning.blogspot.com/2013/09/separating-functions-of-moneythe-case.html

[12] Law, L., Susan S. & Jerry S. (1997). How to make a mint: The cryptography of anonymous electronic cash. *American University Law Review.* 46(4), 1131-1162.

[13] Leemoon, Brian (2017). *Boom or bust, bitcoin a valuation framework.* Wilkes University: Pennsylvania, USA.

[14] Mauss, M. (1990). *The gift: The form and reason for exchange in archaic societies*. Routledge, London.

[15] Miller, M. and Stevens, B. (2002). The future of money. In: OECD, (Ed). *The future of money*, chap. 1, pp.11-30, OECD, Paris.

[16] Mishkin, F. S (2007). *The economics of money, banking, and financial markets* (Alternate Edition). Addison Wesley, Boston.

[17] Money. (2018). *The new palgrave dictionary of economics.* London, UK: Macmillan Publishers Ltd. Retrieved from https://www.palgrave.com/gp/book/9781349951888?countryChanged=true&gclid=Cj0KCQjw2pXXBRD5ARIsAIYoEbd9bV4grFv2x0CQKIxsJ0AdMyygbHVOrCcprWtnTobSwlGAPeiQWbsaAi3TEALw_wcB at 10thApril 2018.

[18] Morgen E. P. (2012). *Bitcoin: The Cryptoanarchists' Answer to Cash*. Retrieved from https://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0

[19] Mougayar, W. (2014). *The 8 identities of bitcoins.* Retrieved from http://startupmanagement.org/2014/02/01/the-8-identities-of-bitcoin/

[20] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash systems.* Retrieved from http://bitcoin.org/bitcoin/bitcoin.pdf at 10th April 2018.

[21] Smithin, J. N. (2000). *What is money?*. Routledge, London.

[22] Sundaram, P. (2016). *Functions of money in the modern economic system.* Retrieved from https://owlcation.com/social-sciences/Functions-of-Money-in-Modern-Economic-System at 10th April 2018.

[23] Swanson, T. (2014). *The anatomy of money-like information commodity: A study of bitcoin.* Retrieved from https://www.amazon.com/Anatomy-Money-like-Informational-Commodity-Bitcoin-ebook/dp/B00MEAO7XK at 10th April 2018.

[24] Szabo, N. (2005). *Bit gold*. Retrieved from https://unenumerated.blogspot.com/2005/12/bit-gold.html at 10th April 2018.

[25] *The etymology of money* (2015). Retrieved from Thewallstreetpsychologist.com. at 24 February 2015.

[26] UK launches initiative to explore potential of virtual currencies. (2014, August 7). *The UK news.* Vol.: 0205/2016. Retrieved from http://www.theuknews.com/news/224504231/uk-launches-initiative-to-explore-potential-of-virtual-currencies.

[27] Vora, G. (2015). Cryptocurrencies: Are disruptive financial innovations here? *Modern Economy*, 6, 816-832. Retrieved from http://dx.doi.org/10.4236/me.2015.67077.

[28] Walker, F. A. (1878). *Money*. New York: Henry Holt & Co.