ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without mentioning the names of the people who made it possible. We are thankful to our guide “Ms. Archana Naik (Prof. CSE Dept)”, whose constructive suggestions and guidance helped us a lot in the case study which we have taken up called as “PAYMENT SOLUTIONS THROUGH BITCOIN”. We would also like to thank our HOD of CSE Dept.”Dr.Tippeswamy M.N”, who gave us constant encouragement and opportunity to work on this project.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **Sl.No** | **Contents** | **Page No.** |
|  | History | 5 |
| 2. | Introduction | 6 |
| 4. | Case Study Scenario | 12 |
| 5. | Technology Used | 13 |
| 6. | Payment Solutions | 23 |
| 7. | Outcomes | 24 |
| 8. | Legality | 25 |
| 9. | Advantages | 27 |
| 10. | Disadvantages | 29 |
| 11. | Analysis | 30 |
| 12. | Conclusion | 31 |

**HISTORY**

In 1983 the American cryptographer [David Chaum](https://en.wikipedia.org/wiki/David_Chaum) conceived an anonymous cryptographic electronic money called [ecash](https://en.wikipedia.org/wiki/Ecash" \o "Ecash). Later, in 1995, he implemented it through [Digicash](https://en.wikipedia.org/wiki/Digicash" \o "Digicash), an early form of cryptographic electronic payments which required user software in order to withdraw notes from a bank and designate specific encrypted keys before it can be sent to a recipient. This allowed the digital currency to be untraceable by the issuing bank, the government, or a third party.

In 1996 the [NSA](https://en.wikipedia.org/wiki/NSA) published a paper entitled *How to Make a Mint: the Cryptography of Anonymous Electronic Cash*, describing a Cryptocurrency system first publishing it in a MIT mailing list and later in 1997, in The American Law Review (Vol. 46, Issue 4).

In 1998, [Wei Dai](https://en.wikipedia.org/wiki/Wei_Dai) published a description of "b-money", an anonymous, distributed electronic cash system.Shortly thereafter, [Nick Szabo](https://en.wikipedia.org/wiki/Nick_Szabo) created "[bit gold](https://en.wikipedia.org/wiki/Bit_gold)". Like bitcoin and other cryptocurrencies that would follow it, bit gold (not to be confused with the later gold-based exchange, [BitGold](https://en.wikipedia.org/wiki/BitGold" \o "BitGold)) was an electronic currency system which required users to complete a [proof of work](https://en.wikipedia.org/wiki/Proof_of_work) function with solutions being cryptographically put together and published. A currency system based on a [reusable proof of work](https://en.wikipedia.org/wiki/Proof-of-work_system#Reusable_proof-of-work_as_e-money) was later created by Hal Finney who followed the work of Dai and Szabo.

The first decentralized cryptocurrency, [bitcoin](https://en.wikipedia.org/wiki/Bitcoin), was created in 2009 by [pseudonymous](https://en.wikipedia.org/wiki/Pseudonymous) [developer](https://en.wikipedia.org/wiki/Software_developer) [Satoshi Nakamoto](https://en.wikipedia.org/wiki/Satoshi_Nakamoto). It used [SHA-256](https://en.wikipedia.org/wiki/SHA-256), a cryptographic hash function, as its [proof-of-work](https://en.wikipedia.org/wiki/Proof-of-work) scheme. In April 2011, [Namecoin](https://en.wikipedia.org/wiki/Namecoin" \o "Namecoin) was created as an attempt at forming a decentralized [DNS](https://en.wikipedia.org/wiki/Domain_name_system), which would make [internet censorship](https://en.wikipedia.org/wiki/Internet_censorship) very difficult. Soon after, in October 2011, [Litecoin](https://en.wikipedia.org/wiki/Litecoin) was released. It was the first successful cryptocurrency to use [scrypt](https://en.wikipedia.org/wiki/Scrypt" \o "Scrypt) as its hash function instead of SHA-256. Another notable cryptocurrency, [Peercoin](https://en.wikipedia.org/wiki/Peercoin) was the first to use a proof-of-work/proof-of-stake hybrid. IOTA was the first cryptocurrency not based on a blockchain, and instead uses the Tangle. Many other cryptocurrencies have been created though few have been successful, as they have brought little in the way of technical innovation. On 6 August 2014, the UK announced its [Treasury](https://en.wikipedia.org/wiki/HM_Treasury) had been commissioned to do a study of cryptocurrencies, and what role, if any, they can play in the UK economy. The study was also to report on whether regulation should be considered.

Bitcoin has been called “digital gold,” and for a good reason. To date, the total value of the currency is close to $112 billion US.

**INTRODUCTION**

**CRYPTOCURRENCY, BITCOIN, TRANSACTIONS :-**

A **cryptocurrency** (or **crypto currency**) is a [digital asset](https://en.wikipedia.org/wiki/Digital_asset) designed to work as a [medium of exchange](https://en.wikipedia.org/wiki/Medium_of_exchange) that uses [strong cryptography](https://en.wikipedia.org/wiki/Strong_cryptography) to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Cryptocurrencies are a kind of [alternative currency](https://en.wikipedia.org/wiki/Alternative_currency) and [digital currency](https://en.wikipedia.org/wiki/Digital_currency) (of which [virtual currency](https://en.wikipedia.org/wiki/Virtual_currency) is a subset). Cryptocurrencies use [decentralized control](https://en.wikipedia.org/wiki/Decentralization) as opposed to centralized digital currency and [central banking](https://en.wikipedia.org/wiki/Central_bank) systems. The decentralized control of each cryptocurrency works through [distributed ledger](https://en.wikipedia.org/wiki/Distributed_ledger) technology, typically a [blockchain](https://en.wikipedia.org/wiki/Blockchain) that serves as a public financial transaction database.

## WHAT IS CRYPTOCURRENCY?

Cryptocurrencies reduced it to a simple definition, is just a limited number of entries in a database no one can change without fulfilling specific conditions. This may seem ordinary, but, believe it or not: this is exactly how you can define a currency.

**BITCOIN**

[Bitcoin](https://en.wikipedia.org/wiki/Bitcoin), first released as open-source software in 2009, is generally considered the first decentralized cryptocurrency. Since the release of Bitcoin, over 4,000 *altcoins* (alternative variants of Bitcoin, or other cryptocurrencies) have been created.Satoshi Nakamoto, the unknown inventor of [Bitcoin](https://blockgeeks.com/guides/what-is-bitcoin-a-step-by-step-guide/), the first and still most important cryptocurrency, never intended to invent a currency.

In his announcement of Bitcoin in late 2008, Satoshi said he developed “A Peer-to-Peer Electronic Cash System” which is completely decentralized.

The single most important part of Satoshi‘s invention was that he found a way to build a decentralized digital cash system. In the nineties, there have been many attempts to create digital money, but they all failed.



After seeing all the centralized attempts fail, Satoshi tried to build a digital cash system without a central entity. Like a[Peer-to-Peer network](https://en.wikipedia.org/wiki/Peer-to-peer_file_sharing) for file sharing.

This decision became the birth of cryptocurrency. They are the missing piece Satoshi found to realize digital cash. The reason why is a bit technical and complex so, let’s try to make it as easy as possible:

*So,in brief, ”* The Bitcoin system enables payments to be sent between users without passing through a central authority, such as a bank or payment gateway. It is created and held electronically. Bitcoins aren't printed, like dollars or euros – they're produced by computers all around the world, using free software.

**In what ways is Bitcoin different from traditional currencies?**

Bitcoin can be used to pay for things electronically, if both parties are willing. In that sense, it's like conventional dollars, euros, or yen, which are also traded digitally.

But it differs from fiat digital currencies in several important ways:

**1 – Decentralization**

Bitcoin's most important characteristic is that it is decentralized. No single institution controls the bitcoin network. It is maintained by a [group of volunteer coders](https://www.coindesk.com/bitcoin-core-roadmap-unveils-signature-optimization-plan/), and run by an open network of dedicated computers spread around the world. This attracts individuals and groups that are uncomfortable with the control that banks or government institutions have over their money.

Bitcoin solves the "double spending problem" of electronic currencies (in which digital assets can easily be copied and re-used) through an ingenious combination of cryptography and economic incentives. In electronic fiat currencies, this function is fulfilled by banks, which gives them control over the traditional system. With bitcoin, the integrity of the transactions is maintained by a distributed and open network, owned by no-one.

**2 - Limited supply**

Fiat currencies (dollars, euros, yen, etc.) have an unlimited supply – central banks can issue as many as they want, and can attempt to manipulate a currency's value relative to others. Holders of the currency (and especially citizens with little alternative) bear the cost.

With bitcoin, on the other hand, the supply is tightly controlled by the underlying algorithm. A small number of new bitcoins trickle out every hour, and will continue to do so at a diminishing rate until a maximum of 21 million has been reached. This makes bitcoin more attractive as an asset – in theory, if demand grows and the supply remains the same, the value will increase.

**3 - Pseudonymity**

While senders of traditional electronic payments are usually identified (for verification purposes, and to comply with anti-money laundering and other legislation), users of bitcoin in theory operate in semi-anonymity. Since there is no central "validator," users do not need to identify themselves when sending bitcoin to another user. When a transaction request is submitted, the protocol checks all previous transactions to confirm that the sender has the necessary bitcoin as well as the authority to send them. The system does not need to know his or her identity.

In practice, each user is identified by the address of his or her wallet. Transactions can, with some effort, be tracked this way. Also, law enforcement has developed methods to identify users if necessary.

Furthermore, most exchanges are required by law to perform identity checks on their customers before they are allowed to buy or sell bitcoin, facilitating another way that bitcoin usage can be tracked. Since the network is transparent, the progress of a particular transaction is visible to all.

This makes bitcoin not an ideal currency for criminals, terrorists or money-launderers.

**4 - Immutability**

Bitcoin transactions cannot be reversed, unlike electronic fiat transactions.

This is because there is no central "adjudicator" that can say "ok, return the money." If a transaction is recorded on the network, and if more than an hour has passed, it is impossible to modify.

While this may disquiet some, it does mean that any transaction on the bitcoin network cannot be tampered with.

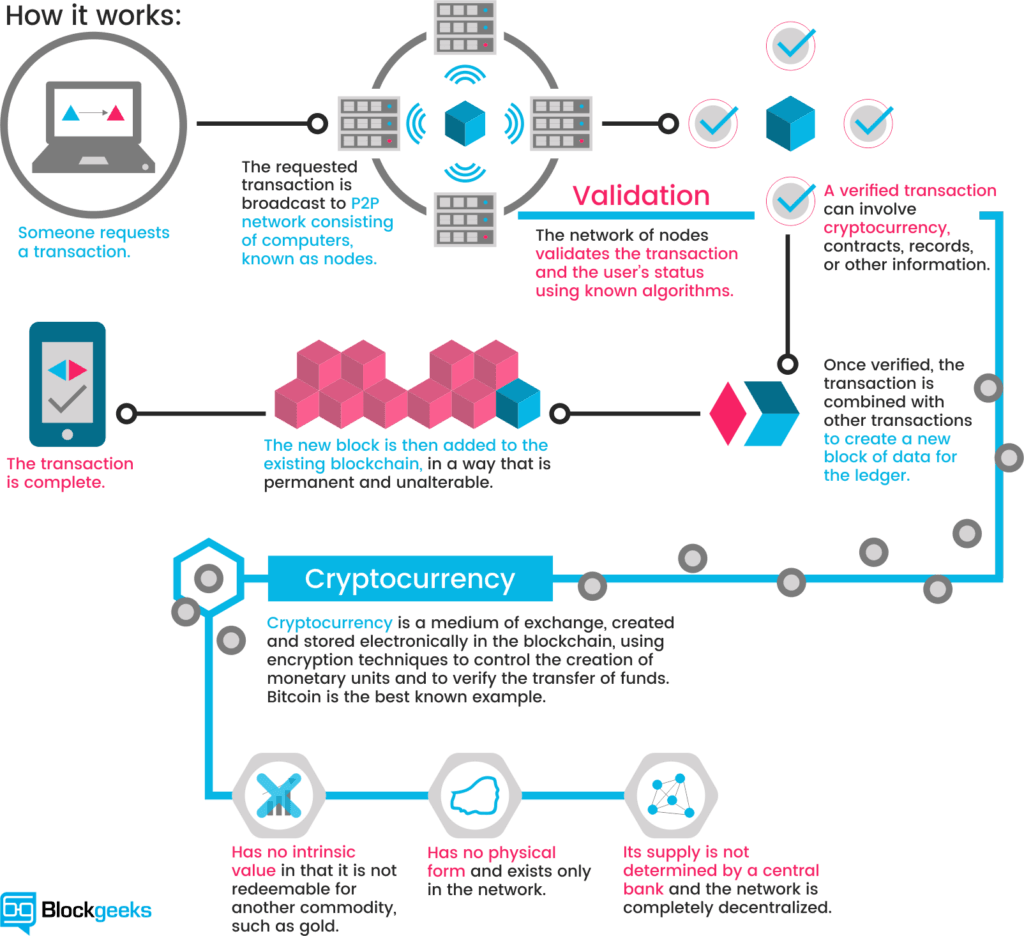
**5 - Divisibility**

The smallest unit of a bitcoin is called a satoshi. It is one hundred millionth of a bitcoin (0.00000001) – at today's prices, about one hundredth of a cent. This could conceivably enable microtransactions that traditional electronic money cannot.

**How it works?**

Let’s have a look at the mechanism ruling the databases of cryptocurrencies. A cryptocurrency like Bitcoin consists of a network of peers. Every peer has a record of the complete history of all transactions and thus of the balance of every account.

A transaction is a file that says, “Bob gives X Bitcoin to Alice“ and is signed by Bob‘s private key. It’s using public key cryptography system. After signed, a transaction is broadcasted in the network, sent from one peer to every other peer. This is basic p2p-technology.



**TRANSACTIONS OR PAYMENTS**

A **transaction** is a transfer of Bitcoin value that is broadcast to the [network](https://en.bitcoin.it/wiki/Network) and collected into [blocks](https://en.bitcoin.it/wiki/Block). A transaction typically references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs. Transactions are not encrypted, so it is possible to browse and view every transaction ever collected into a block. Once transactions are buried under enough [confirmations](https://en.bitcoin.it/wiki/Confirmation) they can be considered [irreversible](https://en.bitcoin.it/wiki/Irreversible_Transactions).

Standard transaction outputs nominate [addresses](https://en.bitcoin.it/wiki/Address), and the redemption of any future inputs requires a relevant signature.

All transactions are visible in the [block chain](https://en.bitcoin.it/wiki/Block_chain), and can be viewed with a hex editor. A [block chain browser](https://en.bitcoin.it/wiki/Block_chain_browser) is a site where every transaction included within the block chain can be viewed in human-readable terms. This is useful for seeing the technical details of transactions in action and for verifying payments.

## Transactional properties:

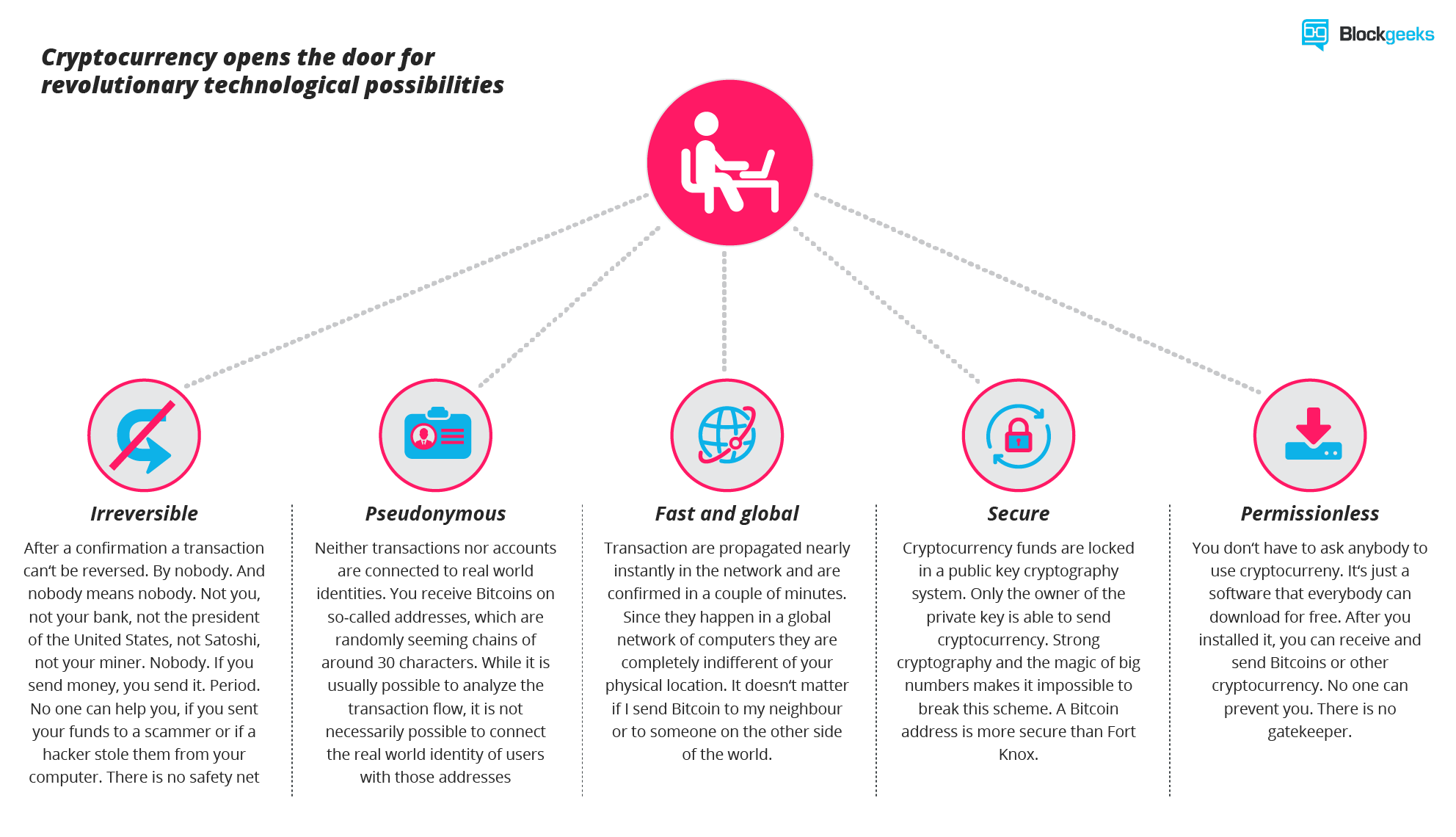
1 **Irreversible:** After confirmation, a transaction can‘t be reversed. By nobody. And nobody means nobody. Not you, not your bank, not the president of the United States, not Satoshi, not your miner. Nobody. If you send money, you send it. Period. No one can help you, if you sent your funds to a scammer or if a hacker stole them from your computer. There is no safety net.

2 **Pseudonymous:** Neither transactions nor accounts are connected to real-world identities. You receive Bitcoins on so-called addresses, which are randomly seeming chains of around 30 characters. While it is usually possible to analyze the transaction flow, it is not necessarily possible to connect the real world identity of users with those addresses.

3 **Fast and global:**Transaction are propagated nearly instantly in the network and are confirmed in a couple of minutes. Since they happen in a global network of computers they are completely indifferent of your physical location. It doesn‘t matter if I send Bitcoin to my neighbour or to someone on the other side of the world.

4 **Secure:** Cryptocurrency funds are locked in a public key cryptography system. Only the owner of the private key can send cryptocurrency. Strong cryptography and the magic of big numbers makes it impossible to break this scheme. A Bitcoin address is more secure than Fort Knox.

5 **Permissionless**: You don‘t have to ask anybody to use cryptocurrency. It‘s just a software that everybody can download for free. After you installed it, you can receive and send Bitcoins or other cryptocurrencies. No one can prevent you. There is no gatekeeper.



For the average person using cryptocurrency is as easy as:

• Get a digital wallet to store the currency.

• Use the wallet to create unique “public addresses” to receive currency.

• Transfer funds in or out of your wallet using public addresses.

**CASE STUDY SCENARIO**

The case study we have taken up is “Payment solutions through Bitcoin”. This case study elaborates in detail how a Bitcoin payment is done, how a single transaction is verified and payment is completed. It also deals with the improvisations we can make in the existing bitcoin transaction mechanism for better and much more secured automated payment solutions.

To realize digital cash we need a payment network with accounts, balances, and transaction. That’s easy to understand. One major problem every payment network has to solve is to prevent the so-called double spending i.e to prevent that one entity spends the same amount twice. Usually, this is done by a central server who keeps record about the balances.

In a[decentralized network](http://blockgeeks.com/guides/what-is-blockchain-technology-a-step-by-step-guide-than-anyone-can-understand/), you don‘t have this server. So you need every single entity of the network to do this job. Every peer in the network needs to have a list with all transactions to check if future transactions are valid or an attempt to double spend.

It’s tempting to think of bitcoin as an account-based system. After all, when I send bitcoin to somebody, that person receives money and I’m left with a remaining balance. In the real world though, things are represented a bit differently. Generally speaking, when I send money to somebody I am sending spending all of that money (minus transaction fees). Some of that money will be spent back to my own personal account if there exists a remaining balance. The point is that all of the money moves every single time.

**TECHNOLOGIES USED**

1. **FORTH PROGRAMMING LANGUAGE**

A script is essentially a list of instructions recorded with each transaction that describe how the next person wanting to spend the Bitcoins being transferred can gain access to them. For this, Bitcoin technology uses forth programming language.

Forth is a simple imperative stack based programming language that processes from left to right. It is intentionally not Turing-complete, with no loops. The spender must provide,

1. a public key that, when hashed, yields destination address D embedded in the script, and
2. a signature to prove ownership of the private key corresponding to the public key just provided.

Scripting provides the flexibility to change the parameters of what's needed to spend transferred Bitcoins.

**2. PUBLIC KEY CRYPTOGRAPHY**

A [Bitcoin address](https://en.bitcoin.it/wiki/Bitcoin_address) is a 160-bit hash of the public portion of a public/private [ECDSA](http://en.wikipedia.org/wiki/Elliptic_Curve_DSA) keypair. Using [public-key cryptography](http://en.wikipedia.org/wiki/Public-key_cryptography), you can "sign" data with your [private key](https://en.bitcoin.it/wiki/Private_key) and anyone who knows your public key can verify that the signature is valid.

1. **ADDRESS RESOLUTION :- HASHING**

To create a bitcoin address, there are various steps. Among all the steps,hashing is done,which can be defined as “the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string”. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value.

* **SHA-256**

SHA-256 is a member of the SHA-2 cryptographic hash functions designed by the NSA. SHA stands for Secure Hash Algorithm. Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. A one-way hash can be generated from any piece of data, but the data cannot be generated from the hash.

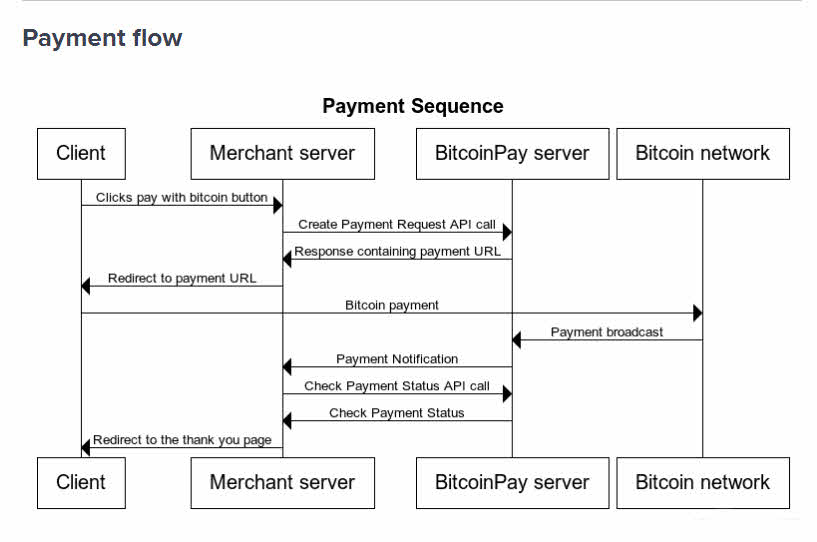
* **RIPEMD-160**

It is a cryptographic hash function based upon the Merkle–Damgård construction. It is used in the Bitcoin standard. It is a a strengthened version of the RIPEMD algorithm which produces a 128 bit hash digest while the RIPEMD-160 algorithm produces a 160-bit output. The compression function is made up of 80 stages made up of 5 blocks that run 16 times each. This pattern runs twice with the results being combined at the bottom using modulo 32 addition.

**3.BLOCK CHAIN**

A **blockchain**, originally **block chain**, is a growing list of [records](https://en.wikipedia.org/wiki/Record_(computer_science)), called *blocks*, which are linked using [cryptography](https://en.wikipedia.org/wiki/Cryptography).[[](https://en.wikipedia.org/wiki/Blockchain#cite_note-te20151031-1) It is "an open, [distributed ledger](https://en.wikipedia.org/wiki/Distributed_ledger) that can record transactions between two parties efficiently and in a verifiable and permanent way".[[7]](https://en.wikipedia.org/wiki/Blockchain#cite_note-hbr201701-7) For use as a distributed [ledger](https://en.wikipedia.org/wiki/Ledger), a blockchain is typically managed by a [peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer) network collectively adhering to a [protocol](https://en.wikipedia.org/wiki/Protocol_(communication)) for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority.

**HOW IT ACTUALLY WORKS?**



Any Bitcoin transaction has three major pieces**: the header, the input and the output**.

**The Header**

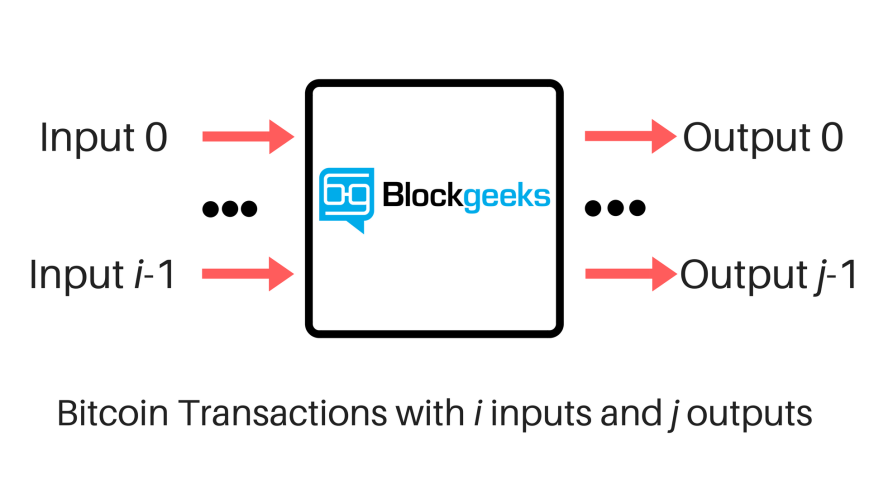
* **hash:** The hash over this entire transaction. Bitcoin generally uses hash values both a pointer and a means to check the integrity of a piece of data. We’ll look at this more in the next section.
* **ver:** The version number that should be used to verify this block. The latest version was introduced in a soft fork that became active in December 2015.
* **vin\_sz:** The number of inputs to this transaction. Similarly, vout\_sz counts the number of outputs. Note that there can be multiple inputs and multiple outputs in any transaction.
* **lock\_time:** We’ll look at this more in later articles, but this basically describes the earliest time at which a block can be added to the blockchain. It is either the block height or a unix timestamp.

**Input**

* **previous output hash:** This is a hash pointer to a previously unspent transaction output (UTXO). Essentially, this is money that belongs to you that you are about to spend in this transaction.
* **n:** An index into the list of outputs of the previous transaction. This is the actual output that you are spending.
* **scriptSig:** This is a spending script that proves that the creator of this transaction has permission to spend the money referenced by receiver.Forth programming comes into picture here.

**Output**

* **value:** The amount of Satoshi being spent (1 BTC = 100,000,000 Satoshi).
* **scriptPubKey:** The second of two scripts provided in a bitcoin transaction, which points to a recipient’s hashed public key.



**STEPS IN A BITCOIN TRANSACTION:-**

Among many methods of transaction, we demonstrate pay to –PK transaction here in our case study.

**STEP 1 :** Validation of my bitcoin

The first step in any bitcoin transaction involves validation of bitcoin. Nodes scan the entire bitcoin network to carry out two things here.

* 1. I have a bitcoin that I can send .
  2. The bitcoin I want to send is not sent to someone else before.

Once this gets confirmed, my transaction gets included in the block which gets attached to the previous block, termed as Blockchain. Note that transactions can’t be undone since it tampers the entire chain.

**STEP 2:** Public and private keys

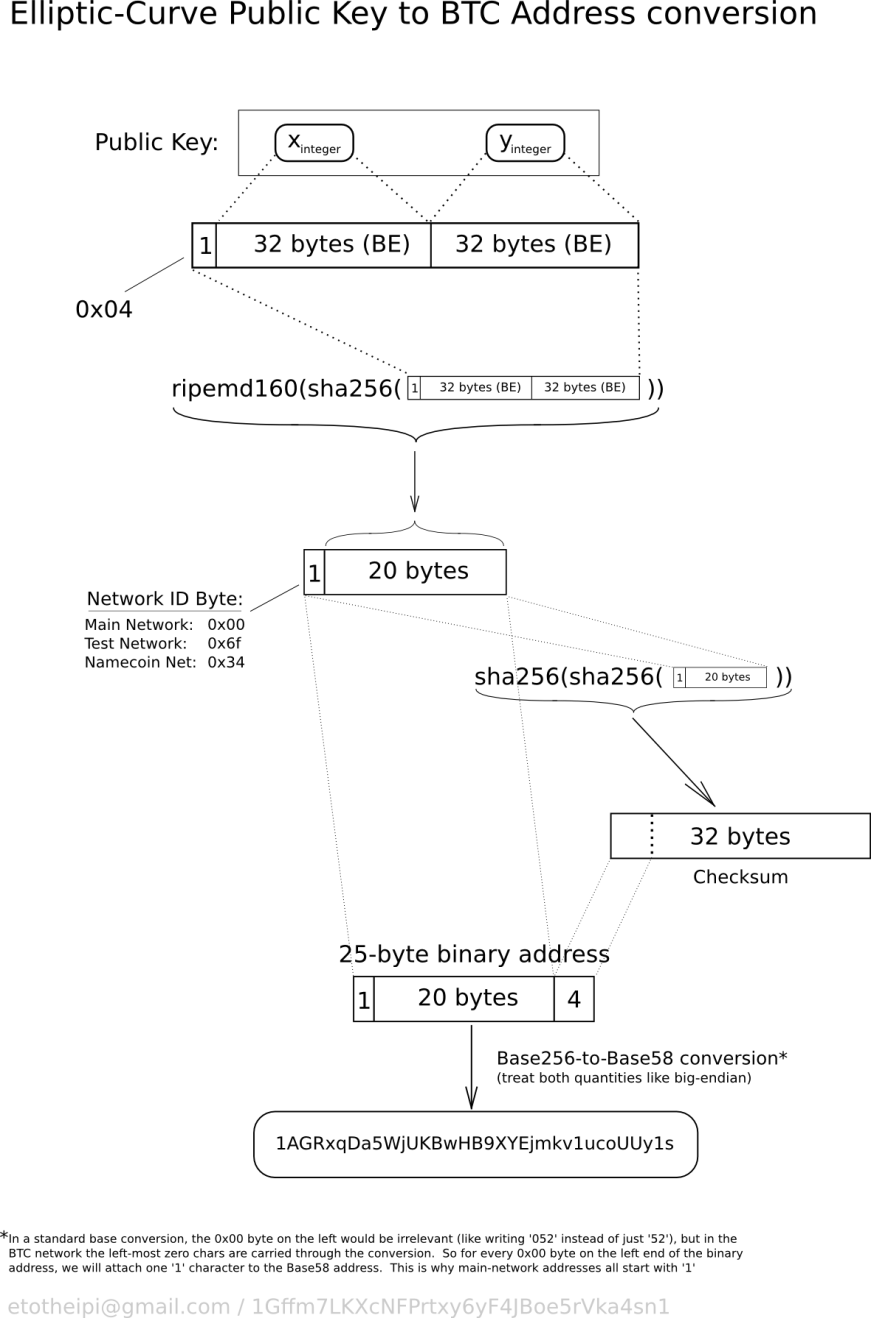
My bitcoin wallet doesn't actually hold my bitcoin. What it does is hold my bitcoin address, which keeps a record of all of my transactions, and therefore of my balance. This address – a long string of 34 letters and numbers – is also known as my "public key. whole world can see this sequence. Each address/public key has a corresponding "private key" of 64 letters and numbers. This is private, and it's crucial that I keep it secret and safe. The two keys are related, but there's no way that you can figure out my private key from my public key.

So, these keys are created before transaction. Note that these keys are hashed.So, there is no way a sender can know the actual public key against a private key. Therefore, the Redeemer specifies both the public key and private key, and the scriptPubKey will duplicate and hash the public key to make sure that the Redeemer is indeed the intended recipient.

**STEP 3:** Address generation

This needs two hashing functions. One is SHA-256 and other is RIPEMD-160. Details of this function gets more complicated. So,lets ssumed that these are used to generate a valid bitcoin address as we see it.

**HOW IT’S DONE?**



A "send" transaction to a specific Bitcoin address requires that the corresponding wallet knows the private key implementing it. This has the implication that if you create an address and receive coins to that address, then restore the wallet from an earlier backup, before the address was generated, then the coins received with that address are lost;

Addresses are added to an address [key pool](https://en.bitcoin.it/wiki/Key_pool) prior to being used for receiving coins. If you lose your wallet entirely, all of your coins are lost and can never be recovered.

Bitcoin allows you to create as many addresses as you want, and use a new one for every transaction. There is no "master address": the "Your Bitcoin address" area in some wallet UIs has no special importance. It's only there for your convenience, and it should change automatically when used

Bitcoin addresses contain a built-in check code, so it's generally not possible to send Bitcoins to a mistyped address. However, if the address is well-formed but no one owns it (or the owner lost their wallet.dat), any coins sent to that address will be lost forever.

0 - Having a private [ECDSA](https://en.bitcoin.it/wiki/ECDSA) key

18e14a7b6a307f426a94f8114701e7c8e774e7f9a47e2c2035db29a206321725

1 - Take the corresponding public key generated with it (33 bytes, 1 byte 0x02 (y-coord is even), and 32 bytes corresponding to X coordinate)

0250863ad64a87ae8a2fe83c1af1a8403cb53f53e486d8511dad8a04887e5b2352

2 - Perform [SHA-256](https://en.bitcoin.it/wiki/SHA-256) hashing on the public key

0b7c28c9b7290c98d7438e70b3d3f7c848fbd7d1dc194ff83f4f7cc9b1378e98

3 - Perform [RIPEMD-160](https://en.bitcoin.it/wiki/RIPEMD-160) hashing on the result of SHA-256

f54a5851e9372b87810a8e60cdd2e7cfd80b6e31

4 - Add version byte in front of RIPEMD-160 hash (0x00 for Main Network)

00f54a5851e9372b87810a8e60cdd2e7cfd80b6e31

*(*note that below steps are the [Base58Check encoding](https://en.bitcoin.it/wiki/Base58Check_encoding), which has multiple library options available )

5 - Perform SHA-256 hash on the extended RIPEMD-160 result

ad3c854da227c7e99c4abfad4ea41d71311160df2e415e713318c70d67c6b41c

6 - Perform SHA-256 hash on the result of the previous SHA-256 hash

c7f18fe8fcbed6396741e58ad259b5cb16b7fd7f041904147ba1dcffabf747fd

7 - Take the first 4 bytes of the second SHA-256 hash. This is the address checksum

c7f18fe8

8 - Add the 4 checksum bytes from stage 7 at the end of extended RIPEMD-160 hash from stage 4. This is the 25-byte binary Bitcoin Address.

00f54a5851e9372b87810a8e60cdd2e7cfd80b6e31c7f18fe8

9 - Convert the result from a byte string into a base58 string using [Base58Check encoding](https://en.bitcoin.it/wiki/Base58Check_encoding). This is the most commonly used Bitcoin Address format

1PMycacnJaSqwwJqjawXBErnLsZ7RkXUAs

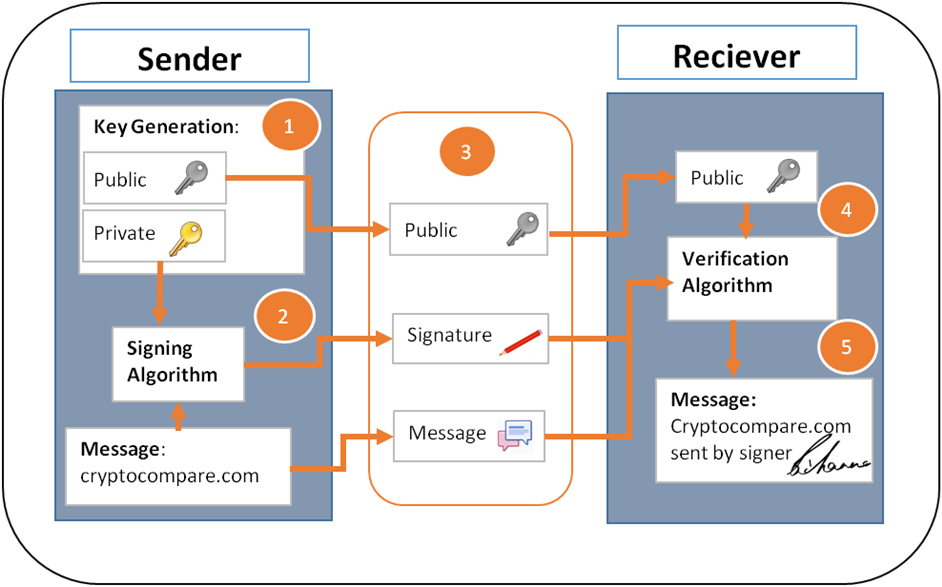
In this way a commonly used address is generated.

There is a possibility that two senders may generate a same address. This phenomena is called as COLLISION. It is highly unlikely if algorithms used are cryptographically strong.

**STEP 4:** SIGNATURE OF KEYS

Any transaction I issue from my bitcoin address needs to be "signed" with my private key. To do that, I put both my private key and the transaction details (how many bitcoins I want to send, and to whom) into the bitcoin software on my computer or smartphone.

With this information, the program spits out a digital signature, which gets sent out to the network for validation.



Both the private and public key are signed into the script that is built in in the software. The node or receiver then checks using the verification algorithm that the message has been signed by the sender, which can only be done by the holder of the private key to the public key that is sent. In scripts, the keys are duplicated and validated. So, it can be confirmed that I own the bitcoin that I am transferring to you, and that I haven't already sent it to someone else – by plugging the signature and my public key (which everyone knows) into the bitcoin program. This is one of the genius parts of bitcoin: if the signature was made with the private key that corresponds to that public key, the program will validate the transaction, without knowing what the private key is.

When all items in our script have been evaluated, our entire script will evaluate to true if true remains on the stack, and false otherwise.

**STEP 5:** BLOCK INCLUSION

Once my transaction has been validated, it gets included into a "block," along with a bunch of other transactions. each block includes, as part of its data, a hash of the previous block. That's what makes it part of a chain, hence the term "blockchain." So, if one small part of the previous block was tampered with, the current block's hash would have to change (remember that one tiny change in the input of the hash function changes the output). So if you want to change something in the previous block, you also have to change something (= the hash) in the current block, because the one that is currently included is no longer correct. Note two things here.

* All of the transaction’s output values are non-negative.
* The sum of this transaction’s input values is greater than the sum of its output values. Note that if the numbers are different, the difference is considered to be a transaction fee that can be claimed by the miner.

The pay-to-PK-hash is a pretty straightforward transaction type. It ensures that only a redeemer with the appropriate public/private key pair can claim and subsequently spend bitcoin.

**SOME PAYMENT SOLUTIONS USING BITCOIN**

## The simplest of all payment systems

Unless a payment needs to be associated with automatic invoices, accepting money is as simple as sending some bitcoin - just display an address or QR code. This simple setup is within reach of almost all users and can fulfill the needs of many clients. From an accounting perspective, it's especially suitable for reducing overhead and adding transparency.

## Many third party APIs

There are many third party payment processing services that provide APIs; you don't need to store bitcoins on your server and handle the security that this implies. Additionally, most of these APIs allow you to process invoices and exchange your bitcoins into your local currency at competitive costs.

## You can be your own bank

If you don't use any third party APIs, you can integrate a Bitcoin node directly into your applications allowing you to become your own bank and payment processor. With all the responsibilities that this implies, you can build amazing systems that process Bitcoin transactions however you would like.

## A new world of possibilities

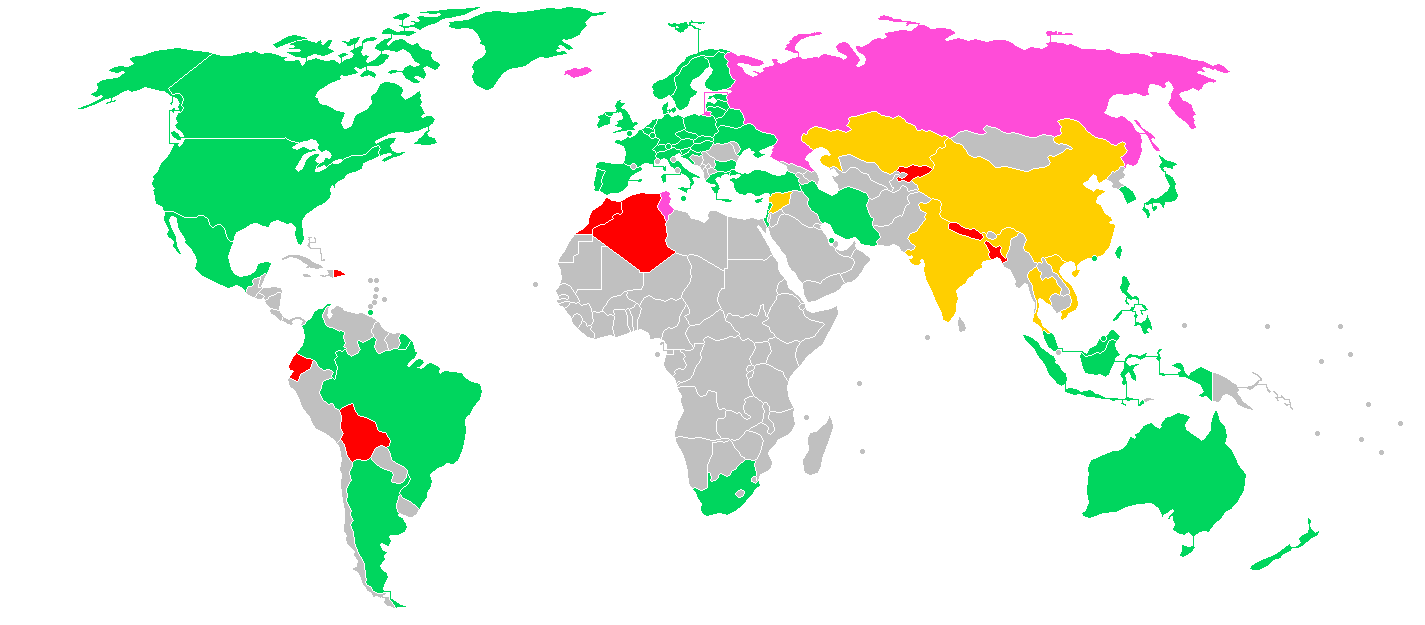
Bitcoin allows you to design new and creative online services that couldn't exist before due to financial limitations. This includes tipping systems, automated payment solutions, distributed crowdfunding services, time locked payment management, public asset tracking, low-trust escrow services, micropayment channels and more.

**OUTCOMES OF THE CASE STUDY**

1. Basic understanding of what a cryptocurrency is.
2. Introduction and a brief study of what a bitcoin is and how it all started.
3. Transaction in terms of a bitcoin and how it is different from normal transaction.
4. Concepts of a block chain and hashing.
5. Implementation of hashing in generating and duplicating keys for validation.
6. Some areas in which application of bitcoin may yield better solutions for persisting systems.

**LEGALITY**

The legal status of bitcoin varies substantially from country to country and is still undefined or changing in many of them.[[1]](https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory#cite_note-1) Whereas the majority of countries do not make the usage of bitcoin itself illegal, its status as money (or a commodity) varies, with differing regulatory implications. While some countries have *explicitly* allowed its use and trade, others have banned or restricted it. Likewise, various government agencies, departments, and courts have classified bitcoins differently. While this article provides the legal status of bitcoin, regulations and bans that apply to this [cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency) likely extend to similar systems as well.



Legal status of bitcoin

**permissive** (legal to use bitcoin)

**contentious** (some legal restrictions on usage of bitcoin)

**contentious** (interpretation of old laws, but bitcoin isn't prohibited directly)

**hostile** (full or partial prohibition)

# **Bitcoins Legal or Illegal in India?**

About bitcoin trading, the RBI apprised of five major risks. The first and foremost is that digital currencies, being in electronic format, are prone to losses arising out of hacking, loss of password etc.

The Indian regulators, starting from the Reserve Bank (RBI) to finance ministry, have been extremely cautious in apprising the investors of the perils of investing money in bitcoins, among other digital currencies.

## This is what the regulators said about the perils of investing in bitcoins:

1. On December 24, 2013, [the Reserve Bank of India (RBI) cautioned](https://www.ndtv.com/business/rbi-warns-bitcoin-traders-of-multitude-of-risks-in-virtual-currencies-1783973) the users, holders and traders of virtual currencies, including bitcoins, about the potential risks that they are exposed to.

"The creation, trading or usage of (virtual currencies) VCs including Bitcoins, as a medium for payment are not authorised by any central bank or monetary authority. No regulatory approvals, registration or authorisation is stated to have been obtained by the entities concerned for carrying on such activities," the RBI had said in a press release issued in the 2013-end.

2. The RBI had stated five major risks of trading in bitcoins. The first is the fact that digital currencies, being in electronic format, are prone to losses arising out of hacking, loss of password etc. The second risk is the lack of any authorized central agency to regulate the payments or to turn to for redressal of grievances. The third is that there is no underlying of asset for VCs, making the value a matter of speculation. Fourth is that the exchanges are located in various parts of the world, making the law enforcement a tricky thing for the multiple jurisdictions available. Fifth is that trading may subject the user to illicit and illegal activities since the VCs, can easily be used for illegal activities anonymously.

3. On February 1, 2017, the central bank again reminded the users of risk involved in bitcoin trading. "The Reserve Bank of India advises that it has not given any licence / authorisation to any entity / company to operate such schemes or deal with Bitcoin or any virtual currency. As such, any user, holder, investor, trader, etc. dealing with Virtual Currencies will be doing so at their own risk," said RBI in the released early this year.

4. On December 5, 2017, the RBI reiterated its warnings in wake of significant spurt in valuation of bictoins. "Attention of members of public is drawn cautioning users, holders and traders of Virtual Currencies (VCs) including Bitcoins regarding the potential economic, financial, operational, legal, customer protection and security related risks associated in dealing with such VCs," said the RBI.

5. On March 15 this year, the finance ministry had constituted an inter-disciplinary committee chaired by Special Secretary in Department of Economic Affairs to take stock of the present status of VCs both in India and globally and suggest measures for dealing with such currencies. The committee comprises nine members including representatives of RBI, SBI, NITI Aayog and Department of Financial Services.

6. In May this year, [the government sought public views on future of bitcoins](http://profit.ndtv.com/news/economy/article-government-seeks-public-views-on-future-of-bitcoin-1696810). Government's official platform MyGov had asked, "Whether Virtual Currencies (VCs) should be banned, regulated or observed?" The comments could be posted before May 31. Nearly 4,000 submissions were made to the government's queries.

7. On June 27 this year, Arun Jaitley held a meeting to examine risks related to virtual currencies (VCs) such as bitcoins. Although several issues concerning bitcoins were discussed, no concrete decision was taken. The meeting was attended by IT minister Ravi Shankar Prasad, NITI Aayog (then) vice chairman Arvind Panagariya, and other senior officials.

8. In the first week of August this year, the inter disciplinary committee submitted its report to the finance minister Arun Jaitley.

9. On the future of cryptocurrencies, [finance minister Arun Jaitley on November 30 said](https://www.ndtv.com/business/crypto-currency-not-legal-in-india-says-arun-jaitley-1782103)that recommendations are being worked at. "The government's position is clear, we don't recognise this as legal currency as of now," Jaitley said when asked whether the government has taken any decision on crypto currency.

10. Income Tax (I-T) [department mulls taxing the gains](https://www.ndtv.com/business/crackdown-at-bitcoin-exchanges-start-five-things-to-know-1787244)made by bitcoin traders and investors as it conducted surveys, on December 13, of exchanges in Delhi, Mumbai, Pune, Bengaluru and Hyderabad.

**ADVANTAGES OF BITCOIN PAYMENTS**

* **User Anonymity**

Bitcoin purchases are discrete. Unless a user voluntarily publishes his Bitcoin transactions, his purchases are never associated with his personal identity, much like cash-only purchases, and cannot be traced back to him. In fact, the anonymous Bitcoin address that is generated for user purchases changes with each transaction.

* **No Third-party Interruptions**

One of the most widely publicized benefits of Bitcoin is that governments, banks and other [financial intermediaries](https://www.investopedia.com/terms/f/financialintermediary.asp) have no way to interrupt user transactions or place freezes on Bitcoin accounts. The system is purely peer-to-peer; users experience a greater degree of freedom than with [national currencies](https://www.investopedia.com/terms/n/national-currency.asp).

* **Purchases Are Not Taxed**

Since there is no way for [third parties](https://www.investopedia.com/terms/t/third-party.asp) to identify, track or intercept transactions that are denominated in Bitcoins, one of the major advantages of Bitcoin is that [sales taxes](https://www.investopedia.com/terms/s/salestax.asp) are not added onto any purchases.

* **Very Low Transaction Fees**

Standard [wire transfers](https://www.investopedia.com/terms/w/wiretransfer.asp) and foreign purchases typically involve fees and exchange costs. Since Bitcoin transactions have no intermediary institutions or government involvement, the costs of transacting are kept very low. This can be a major advantage for travelers. Additionally, any transfer in Bitcoins happens very quickly, eliminating the inconvenience of typical authorization requirements and wait periods.

#### Control and Security

* Allowing users to be in control of their transactions help keep Bitcoin safe for the network.
* Merchants cannot charge extra fees on anything without being noticed. They must talk with the consumer before adding any charges.
* Payments in Bitcoin can be made and finalized without one’s personal information being tied to the transactions.
* Due to the fact that personal information is kept hidden from prying eyes, Bitcoin protects against identity theft.
* Bitcoin can be backed up and encrypted to ensure the safety of your money.

**Mobile Payments**

Like with many online payment systems, Bitcoin users can pay for their coins anywhere they have Internet access. This means that purchasers never have to travel to a bank or a store to buy a product. However, unlike online payments made with U.S. bank accounts or [credit cards](https://www.investopedia.com/terms/c/creditcard.asp), personal information is not necessary to complete any transaction.

**DISADVANTAGES OF BITCOIN PAYMENTS**

#### Lack of Awareness & Understanding

* Fact is many people are still unaware of digital currencies and Bitcoin.
* People need to be educated about Bitcoin to be able to apply it to their lives.
* Networking is a must to spread the word on Bitcoin.
* [Businesses are accepting bitcoins](https://coinreport.net/accepting-bitcoin/) because of the advantages, but the list is relatively small compared to physical currencies.

#### Risk and Volatility

* Bitcoin has volatility mainly due to the fact that there is a limited amount of coins and the demand for them increases by each passing day.
* However, it is expected that the volatility will decrease as more time goes on.
* As more businesses, medias, and trading centers begin to accept Bitcoin, its’ price will eventually settle down.
* Currently, Bitcoin’s price bounces everyday mainly due to current events that are related to digital currencies.

#### Still Developing

* Bitcoin is still at its infancy stage with incomplete features that are in development.
* To make the digital currency more secure and accessible, new features, tools, and services are currently being developed.
* Bitcoin has some growth to do before it comes to its full and final potential.
* This is because Bitcoin is just starting out, and it needs to work out its problems just like how any currency in its beginning stage would need to.

**No way to reverse the payment**– If you mistakenly pay someone by using cryptocurrency, then there is no way to get a refund of the amount paid. All you can do is to ask the person for a refund and if your request is turned down, then just forget about the money.

**Uncertainty & Volatility**– Since cryptocurrencies are so new, they are also very volatile. This is one of the main reasons mass adoption is taking longer than it should. Many corporations don’t want to deal with a form of money that is going to go through huge swings in volatility.

**Scaling** – Based on the way *smart contracts* are designed, there is a limit to the speed and number of transactions it can process at a time which has hindered the widespread adoption of digital currencies. With the introduction of [*Lightning Networks*](https://coinpupil.com/altcoins/lightning-network-bitcoins-scaling-solution/), the crypto community has put a foot in the right direction which gives breathes hope into the idea that cryptocurrency could one day replace conventional credit card transactions.

**ANALYSIS**

Though cryptography and cyber security is a new concept for all of us, this case study has paved a way to take interest and acknowledge the importance of applications of this subject. Bitcoin being the biggest application of cryptography and cryptocurrency was always a keen topic to study. This case study made us to learn how it actually works, the technology behind bitcoin payments and the hype of it in the market. We also, at the end understood how are the possible ways of improving payment solutions for existing systems through bitcoin. Cryptographic algorithms and usage of SHA-256 and other hashing methods was a real application of what we are studying. Working in a team also improved our team skills, made realize our self potential and participate in a bigger task. In short, this case study was both informative, exciting and a learning aspect for our future studies om cryptography.

**CONCLUSION**

As of now, Bitcoin as payment option has no significant reception which is a major drawback but slowly and steadily it is consolidating its position. Both developed as well as developing countries are legalizing and regulating the use of cryptocurrency in some way or another. Even countries with a high political restriction like Russia and China are trying to make it so people can be able to freely spend them. We can already see Bitcoins effect on the economy. It is very large and only growing at an outstanding rate.

Singapore and Switzerland are the most advanced countries in the use of cryptocurrency as of now. Clearly, the advantages do overcome the disadvantages and this is the reason why the base of cryptocurrency is increasing. After seeing the benefits of using cryptocurrency, people are more than willing to accept the risks involved. This article will help you to form a better perspective on its use. Like anything else, there are few shortcomings but the positive aspects outshine the drawbacks.

With everything in life, there are always pros and cons and this is why you need to weigh both actions thoroughly before making a decision. For cryptocurrency, it’s ascension has been due to its ability to initiate secure and untraceable transactions. Now, that the technology is here, only time will tell if the rest of the world will accept it.