To

Mining

Bitcoins

- An introduction to the concept of currency
  - Introduction to Bitcoin
  - Definitive guide to mining Bitcoins
  - Trading Bitcoins
  - Accepting payments on your site via Bitcoins
  - Alternatives to Bitcoins
  - Bitcoins in India
  - Important DOs and DON'Ts
  - Future of Bitcoins and alternative currencies
Join the forum to express your views and resolve your differences in a more civilised way.

Post your queries and get instant answers to all your technology related questions.

One of the most active online technology forums not only in India but worldwide.
MINING BITCOINS
An introduction to the concept of currency
Before getting into Bitcoins, you must first understand how regular money works. This chapter is your cheat-sheet to practical economics.

Introduction to Bitcoin
For those of you who’ve never heard of Bitcoin before, we will take a walk-through of its entire system, one step at a time.

Definitive guide to mining Bitcoins
In order to spend Bitcoins you need to have some and getting your hands on a few can be quite the task, we take you through the process and let you know the easiest way to go about it.

Trading bitcoins
This new crypto-currency doesn’t adhere to the normal system that we have in place. Read on to learn how to perform Bitcoin transactions.
Accepting Bitcoin payments on your website

The Bitcoin economy operates in the billions with multimillion dollar USD transactions happening everyday so it’s only prudent that you incorporate this medium into your business.

Alternatives to Bitcoins

Ever since Bitcoin hit the scene nearly 70 other cryptocurrencies have gone into circulation. We take a look at the biggest ones.

Bitcoins in India

As the rest of the world deals with the impact of the rise of digital currencies, India is not far behind. We take a look at the equation of Bitcoin with India.

Important DOs and DON'Ts

The Bitcoin world is a dangerous place and many precautions are needed to make sure that your money is safe. In this chapter we give advice on how to manage your Bitcoins.

Future of Bitcoins and alternative currencies

Is Bitcoin the end of the line for virtual currencies or just the beginning? We play soothsayer in this final chapter and try to predict the future.
Introduction

Bitcoin? Virtual Money? Revolution? Stop! What’s going on here?

Who could have predicted ten years ago that a virtual currency system designed by an anonymous figure from the internet would suddenly become an issue for international economies? Well, we tried our best but as 2013 demonstrated, Bitcoin and the world of virtual currencies are a roller coaster ride of the unpredictable.

As newspapers the world over start carrying stories about Bitcoin and moving them from the technology pages to the finance pages, many people across the globe wait for Bitcoin to become truly mainstream. Even Indian innovators are showing interest in the Bitcoin phenomenon and attempting to bring it to the common consumer. However, faced with government restrictions and murkiness about how the Bitcoin system works they are faced with many obstacles.

The Bitcoin system is a relatively new phenomenon and it offers many rewards for participants at different levels - from those who simply use it as a currency to those who wish to become an integral part of its mining community. And as this system continues to operate we will discover its many flaws and strengths. It’s very likely that the Bitcoin of today will undergo many changes in the years to come but it is our undisputed belief that Bitcoin is sure to become part of the future internet.

This issue of Fast Track seeks to cover the broad range of questions that face you, our readers, regarding the different aspects of Bitcoin and how you can be a part of it.
We take you through a variety of levels in this issue without limiting it to a simple FAQ about the Bitcoin technology. The chapters are designed to educate, inform and advise in equal measure without advocating for or against Bitcoin.

We recognise that Bitcoin can’t be dealt in isolation as a technological device without placing it context with its impact on the world. Bitcoin is designed to be a currency like banknotes and coins. It differs from online payment mechanisms like PayPal and credit cards in many ways. To understand its role in the real world of everyday finance we begin with an explanation of currency and then move to an explanation of Bitcoin itself.

We then walk you through the technical aspects of the Bitcoin system which includes how you can make your own Bitcoins. The rest of the chapters take a look at the world built around Bitcoin, including topics of alternative digital currencies like Bitcoin, the dangers of using Bitcoin and we end with our own prediction of what you can expect in the future from the Bitcoin phenomenon.

We hope this issue of Fast Track on Bitcoin will make you more sure than ever before of how you see this innovative new technology as a part of your life.

We look forward to hearing your views and feedback at: editor@thinkdigit.com about this Fast Track.

Disclaimer: This Fasttrack aims to introduce readers to the various processes involved in bitcoin mining. Understand that as with anything of a speculative nature, there are a number of risks associated. No part of this FT should be construed as financial advice. Proceed at your own risk.
Before getting into Bitcoins, you must first understand how regular money works. This chapter is your cheat-sheet to practical economics.
Bitcoin is perhaps one of the most exciting innovations of the modern digital age. But before we dive deep in to the notorious world of this digital crypto-currency let us sort through the necessary fundamentals of the world it is prophesied to change - currency.

**Money vs. Currency**

Is there really a difference between money and currency? Well yes - a significant difference. Money is the general term used for any commonly accepted “medium of exchange”. Money can exist in any form - most commonly an object or maintained record of transaction which is acceptable by the significant majority of people as payment for goods and services. Currency on the other hand is the name for the commonly accepted form of money that is in circulation. In most cases currency is represented as banknotes and coins but its definition can also encompass anything that is commonly held to represent value and is accepted on those terms.

In everyday speak money and currency are interchangeable terms however in precise usage it’s important to note the difference, e.g. Barney Stinson has a lot of money but if he buys a suit in Italy he better make sure he has the right currency (Euro).

Money is therefore the broader term used to talk about wealth, value and the ability to acquire goods and services. Having a lot of money is good, but having a lot of any currency depends on what the currency is - for instance its better to have one United States dollar as currency than ten thousand Indonesian Rupiah as currency.

Historically, money has found many forms in societies and economies, from a simple honour bound promise between ancient farmers (“I owe you”) to the hard cold cash of today. Interestingly, the evolution of the “I owe you” essentially gave birth to “I owe you one unit of…” - that blank space was filled with many different things over time including - grains, cattle and shells - all of which were valid money currencies of their time. However as societies grew and began trading with other societies the need for a universal “store of value” gave birth to minted money that was based on precious metals i.e. gold and silver.

Within the modern context currencies have continued to evolve (as with the creation of the Euro) but money has, for the longest time, held certain fixed features; to be a medium of exchange, a unit of account and a store of value. However, in the post-modern digital age, currencies such as Bitcoin are even testing these features.
What is currency?
Currencies are rigidly defined by the systems or economies they are commonly used in society. In the modern economic usage, they are primarily “stores of value” - which means that they assure all users that they are worth having due to their assured value. Although the degree and relative nature of that value may differ, it is stable and generally known. E.g. the Indian rupee is an assurance of value in the Indian system but it may not be easily used in China, but it can be traded for Chinese currency of equal value through established systems.

All across the world the different currencies are traded on foreign exchange markets under the careful watch of government regulations. Since each currency is established and regulated by national governments, they represent the economic power and stability of the nation's economy and require monitoring. As recent international economic developments have shown, the economic strength of any nation is first felt in the strength of its currency.

Some currencies, such as the United States dollar, are near-universally accepted across the world due to the relative strength of its national economy, whereas the former (2009) currency of Zimbabwe ran out of steam with a 100 trillion dollar note that was even then less valuable than one US dollar. Currencies are constantly changing in value across markets as countries continue to trade with each other but there are a handful of currencies that are broadly accepted - the Euro and US dollar - being the preferred ones.

Due to the nationally critical nature of this form of money, currencies are produced under extremely controlled setups by governments. Often
times these currencies, usually in the form of banknotes, function as a written statement of promise or contract between governments and those who possess the notes. This can be seen on the Indian currency with the words - “I promise to pay the bearer the sum of X rupees” - which is signed by the Governor of the Reserve Bank of India. The currency in this sense functions as a bond of trust, which is key assurance of value that national currencies enjoy.

**History of Value in Currency**

Currencies as stores of values are critical for national and international economies. But the question of their value is constantly under debate. What makes the US dollar so much more valuable when compared to the Somali shilling (15,000 Somali shillings for 1 USD in May 2013)? Where do currencies get their value from? To first understand the notion of value it is important to note the history of money and nations.

The early form of money that found widespread acceptance was in the form of precious metals - gold and silver. The desirability of these metals across diverse cultures made them the ideal medium of stored value. Traders from different parts of the world could securely trade goods and services for pieces of gold and silver. But as the scale of trade increased across distances and quantity it wasn’t practical or safe for traders to carry around hundreds or thousands of valuable metal pieces with them. They were just too heavy.

In order to simplify this problem without disrupting trade the concept of “notes” was created. First used in 8th century China, a piece of paper was created to represent the value of the metal coins that were to be traded. However these “notes” needed to be guaranteed by a trustworthy party, which is where banks came into existence. Traders usually travelled back and forth between fixed locations and made diverse trades with many people. So banks would hold the coins for traders and issue them “notes” that were accepted by other parties who trusted the banks. The building of trust was therefore the banks job and this led to banks having branches in various cities so they could process trade.

Trader A would typically deposit X number of coins in a bank and receive a “notes” of that value. When making a trade, A would pay Trader B using the “notes” issued to him by the bank in his city. When trader B went to trader A’s city the same note could be used to pay. As long as all parties involved trusted the bank trade could carry on. Over time this system became more efficient to account for various possibilities such as “what if trader B didn’t go
An introduction to the concept of currency
to trader A’s city” and so forth. The solutions of these types of issues led to the modern economy where nations and banks were entrusted with guaranteeing the value of “notes” or currency as they became over time.

For the longest time all currency issued by nations was guaranteed by deposits of gold in their reserves. The assurances printed on currency notes such as “I promise to pay the bearer a sum of X...” meant that an individual could theoretically go to the national reserve and exchange the “note” currency with X value of gold. However, this was rarely ever done or necessary and the international economies continued to move on trust - of the fact that there actually was gold of equal value in the reserves. This was known as the “Gold Standard” and was formally entered into by 44 nations in 1944 as a part of a new international economic system that would allow global trade. This decision was taken at the United Nations Monetary and Financial Conference or the Bretton Woods Conference. The agreement also gave birth to the International Monetary Fund (IMF) and the International Bank for Reconstruction and Development (IBRD). Currencies were tied to the U.S. dollar and the IMF managed any intermittent imbalances of payment between nations.

This form of currency system in domestic and international economies found value from its gold reserves. As long as gold remained a valued commodity, the currency representing it was considered valuable. Clearly this proved harder to apply in the long run than it was initially thought. The necessity of having an equal amount of gold in reserves forced banks and nations to keep accumulating the metals as currency demand increased. And the use of gold and silver in industrial processes’ became a far more pressing concern since you could either store the metal as reserve for currency or lose it in an industrial process. The pressure on maintaining enough reserves as populations and currency demand increased became a problem.
At first the solution to the problem was simple - to break its own rules. Instead of maintaining a 1:1 ratio In order to replace the hard to manage metal, the value of trust became more important. It no longer mattered if there was enough gold or silver to represent the currency value, what mattered was if everybody was still willing to accept the currency itself. And as long as the currency was backed by a sovereign nation and government that was trustworthy trade could continue. This realisation eventually led to the abolishing of the gold standard by US President Richard Nixon at the 1971 meeting of the Bretton Woods Conference. The United States ended its USD to gold convertibility and declared the dollar to be a fiat currency which essentially led the US dollar to replace gold in the reserves of most countries.

So to the question of what gives currency its value - the trust of its users and its continued demand. Trust and demand. As long as something, anything - oil, gold, pieces of specially stamped paper, digital currency - is in demand it will have value. In the modern economy the one object that was the widest possible demand is currency - some more than others. And the reason behind that demand is the inherent trust of the users that everyone else also wants it. Any currency would be useless if nobody wanted it. It seems like a strange trick but it’s the foundation of modern economics.

As long as enough people believe in the value of money the global engine of trade keeps on running. If suddenly people lost faith in the value of currency it would be nothing more than bits of paper and metal. As long as this dual coincidence of wants remains in an economy currencies will always have value. Of course, the relative value of currencies differs - since that is based on a multitude of factors - the biggest one being the demand of the currency itself. The reason the US dollar is considered most valuable is because it is the one currency that is globally in demand.

This strange circular logic of coincidental wants grew from a more rational foundation - that after the Second World War the only country that was prosperous in the world was the United States. Most nations were indebted to it in huge amounts or had been devastated by the war.
An introduction to the concept of currency

This tangible advantage allowed the US currency to reflect the strength of its nation and since then has continued to (through controversial means) remain the most powerful currency in the world as well as the most valuable.

**Who controls currency?**

As we’ve discussed, currency is a representation of national wealth, power and value. It derives its value from trust and trade utility. But in order to administer its flow across borders and within nations a system is necessary. This system is part of every country’s setup and is known as the central bank. And the institution that coordinates and administers the planning of these many central banks is the Bank for International Settlements (BIS) in Basel, Switzerland. However, the BIS has no direct control over the currencies of various nations and is involved only in monetary policy guidelines that its 58 member nations have to adhere.

Although the BIS is an important part of the international network of trading economies the actual control over currency comes from the specific central banks and national monetary policies of economies. Currency or “minted” money i.e. notes and coins, is manufactured by governments of nations through monetary policy enforcement that allows them to introduce increase the “money supply” in their economies. This process is highly sensitive as the rampant creation of currency can destabilize economies and is done with great care and timing. It is a necessary part of managing a nation’s monetary policy and is therefore very carefully administered.

Changes of lower impact such as the introduction of new coins or notes and the erasure of older denominations of currency are occasionally necessary to keep up with market forces such as inflation. Other ways of controlling currency in a national economy such as devaluation and redenomination are also strictly in the realm of governmental economic policy. Any changes to a national currency are a complex and fairly transparent process
in most countries. This exposure limits the volatility with which changes can be made to manipulate the appearance of an economy. The control over currency isn’t as direct as some people might fear.

**How does a currency’s value change?**
The value of all currencies is in constant fluctuation but usually within a very finite range. In the course of a day the value of the Indian rupee rarely fluctuates beyond tens of paise and is the general reflection of the impact of demand and supply on the currency due to ongoing trade. The changes in value of a currency brought on by these trade or market forces is considered completely natural and fair. The best means for a currency to remain valuable is to ensure that other nations require the domestic currency to make trade.

A simple example is as follows - an Indian wants to buy a car from America. To do so she will have to make the payment in US dollars since no American car company will accept Indian rupees (since no one sells anything in America in exchange for Indian rupees). In order to obtain the dollar the Indian will trade her rupees for dollars from a currency exchange and make the payment. This increase in the demand for the dollar will make it stronger and increase its value. However, if an American wants to procure the services of Shah Rukh Khan, she will similarly have to trade her dollars for rupees, which in turn would increase the value of the rupee. As long as the demand for American goods outweighs Indian goods between the two countries, the rupee will never be as strong as the dollar. But if suddenly India is selling more goods to America than buying from America, the Indian rupee will get stronger and more valuable. This fluctuation in the trade between not just two nations, but many nations in various permutations and combinations in an ongoing non-stop flow causes the currency’s value to change. The simplest way for a nation to positively affect the value of its currency is to increase its demand by exporting more goods and services to other nations.
Conversely, when any nation's productivity is hampered and it ends up importing more than exporting, the value of its currency is weakened. It's interesting to note that in 1966 the value of a US dollar in Indian rupees was 7.5:1 and is currently (January 2014) around 61:1. This reflects how the balance of trade between the two nations can broadly be considered.

Other ways of changing the value of a currency lie in the hands of the government and the central banks of nations. As mentioned earlier, changing monetary policy to increase or reduce currency supply can also have an effect on the value. In addition to which practices of devaluation can also cause changes in value. Devaluation is the monetary policy whereby the government or the central bank intentionally decreases the exchange rate of its currency with another currency. The reasons behind why this is done are mostly to do with the management of lagging trade and struggling economic development, and the currency devaluation is a tool used to manage the problem. However any move to do so is usually seen as a panic indicator and causes more problems than its fixes.

**How is currency power?**

The world is a much smaller place than it was a hundred years ago, especially in economic terms. Never before was it possible for an Indian tea farmer in West Bengal to purchase a cell phone designed by engineers in America and assembled by workers in China, that was marketed to him via professionals in India based on an international advertising campaign created in London. And customer service in his own district of Jalpaiguri.

The reason the international system of trade is able to sustain itself is due to the commonly held belief that all currency has value - some more than others but value nonetheless. And by trading currency for goods and services in multilateral ways across various nations can an efficient system of resource management be created which results in better products and services at the most competitive prices. However, all this is easier said than done.
The real world behaviour of people in this system is oriented towards winning, not towards fairness or efficiency. A major example being the spending of hundred of millions of US dollars annually by competitors like Pepsi and Coke to promote their product over the other when essentially they are both carbonated sugar water - not very efficient and yet very necessary if they wish to remain profitable. This conflict between the design of international economies and the private players who operate within them makes currency the source of all power.

A nation may choose to orient its power in different ways but the end goal is the same - to retain an advantage over other nations in the economic exchange. The work towards this advantage nations need to make products and services flow out of there country in a higher ratio than they flow into the country. By maintaining this balance of exchange they can increase the demand of their currency and directly have more power. Since the end of the last world war, most of the world has imported from countries such as America and Middle-Eastern oil nations. Only since the ‘90s has widespread globalisation allowed a wider exchange between countries but the advantage is already in the favor of select nations.

From making purchases of everyday items to starting a new business, the reality is this - currency is power because it allows you greater freedom and liberty in fulfilling your desires.

Glossary of Money - We'll briefly explain the meaning of certain terms that will assist in understanding the concepts around money and currency more clearly.

**Fiat currency or fiat money**
The word “fiat” is latin and means “it shall be”. In connection with currency it is the term used to describe any form of money that is under the control of a government and is considered a legal tender. Fiat currency or fiat money
An introduction to the concept of currency is produced, controlled and managed by national governments and unlike gold or silver currency has no intrinsic value. For example, a 100 rupee note is not produced from materials that are valued the same as its face value but is valued because it is a fiat currency supported by the government.

Veil of money
Almost all forms of modern currency are fiat currencies or currencies dependent on fiat currencies. The veil of money relates to the question of whether money itself is like other commodities (like gold) or does it have any intrinsic quality of its own. Over time this theory has gone from saying that money by itself is useless and is only of value in exchange of actual goods or services to the current belief that it is simply a store of credit and holds value when it is treated as valuable. In economic studies it takes on a more technical meaning related to interest rates and monetary policy by the government.

Central banks
A central bank or reserve bank is the main authority within a nation that manages a country’s money supply as well as its production and manipulation through interest rates and other enforcements of monetary policy. It is created to administer and guide the commercial banking activities in a country along with the power to penalise and punish fraudulent acts. They are not directly controlled by government agents and function with a mixed authority from the executive and legislative branches of government. In India, the Reserve Bank of India has this duty.

Tinkerbell effect
The Tinkerbell effect gains its moniker from a character in the play Peter Pan, where a fairy - Tinkerbell - exists only as long as people believe in the existence of fairies. The similar association is made in economics between money and its value. Money is valuable as long as people continue to believe that it has value.

Friedman rule
The Friedman rule is a technical concept in monetary policy, named after economist Milton Friedman. The rule is meant to define an association between interest rates set by central banks and the money supply in the market. The rule says that the interest rate should be such that the money
An introduction to the concept of currency

held by persons would retain its long term value and not depreciate. By balancing the central bank interest rate with the rate of currency deflation, a nominal interest rate of zero could be achieved. This is an ongoing debate depending on various factors of an economy intended to outline the ideally preferred scenario.

Money illusion

This term defines the conceptual flaw in thinking when referring to the value of money over time. A simple example is that if the price of an ice cream in year 2000 was 10 rupees, the expectation in the minds of people is that it will continue to be 10 rupees in 2014 even though the value of the 10 rupees has reduced since 2000. That is, the face value of money is mistaken as its real value or purchasing power. However, as we know since fiat currencies have no intrinsic value, the face value of currency can remain the same while its real value continuously fluctuates. People continue to not recognise this in certain situations - a common example being when in experiments they consider a 2 percent reduction in income with steady prices as unfair but consider a 2 percent increase in income with 4 percent inflation as being fair, even though both scenarios are mathematically identical.

RBI – the only bank in country which doesn’t take deposits or issue cash to people.
INTRODUCTION TO BITCOIN

For those of you who’ve never heard of Bitcoin before, we will take a walk-through of its entire system, one step at a time.

We now take a look at Bitcoin - its origins, history and its supposed promise of liberty in the digital age.

What is Bitcoin?
Bitcoin is the most widely used peer-to-peer distributed decentralised digital currency in the world. The currency is based on the Bitcoin protocol that allows digital currency (Bitcoins) to be securely, efficiently and quickly transferred between people. It is a widely accelerating form of digital cash
Introduction to Bitcoin

that can be used to make online payments for products and services, as well as regular transfers of cash between people. It is also traded online, like fiat currencies, in an online currency exchange known as Mt. Gox.

What is a digital currency?

It's important to understand the term digital currency to understand Bitcoin's role as a currency. Digital currency or electronic money, exists as an alternative to normal currency and has seen various forms over the past few years. As of yet, it has not found any national or institutional backing across nations and has only been experimented with in smaller communities.

Other forms of virtual currencies like in-game money or closed system currencies are only valuable within the confines of their systems in virtual economies. Bitcoin as a digital currency has found the widest acceptance to use for real world goods and services without virtual world limitations.

The most conventional form of digital currency has come to include web-based wire transfers, machine withdrawals, online credit card use and digital bill payments that use electronic means to make payments. However, these are based on a very broad definition of digital currency that is simply an extension of the traditional economic system (system of exchange) that is still rooted to fiat currencies and only transfers records of credit and dues using the internet as a communications protocol.

Decentralised and Crypto

Two key features of Bitcoin as a successful digital currency are - decentralisation and cryptography. Unlike fiat currencies or theoretical fiat digital currencies, Bitcoin is decentralised, which basically means that it isn't regulated or managed by a single institution or person. Bitcoin is based on a peer-to-peer distributed network and regulated by an open source network system that regulates the production of Bitcoins on a clearly understood and transparent logic.

Since there is no single authority behind Bitcoin's management the fear of currency manipulation through increased production or institutional devaluation is removed. This allows the adoption of the currency to be more welcoming as users don't have to have trust in a bank or agency, but in the system itself that ensures no means of external manipulation.

Bitcoin is also a cryptocurrency which makes it an ideal digital medium of exchange as compared to other virtual currencies. It is also the first
cryptocurrency to be so widely traded and adopted. The security of the open source code has been thoroughly tested and improved over time to ensure that it can’t be “hacked”. Cryptographic principles are also used in order to regulate the mining of the currency as well as its authenticity. The possibility of digital counterfeiting is completely moot due to the system’s design.

In conjunction to the cryptographic principles involved in its production, Bitcoin is also administered in a decentralised network that can authenticate the validity of all Bitcoins produced using user keys and signatures in a distributed online registry, which ensure that duplication of transactions does not happen and frauds are avoided.

The nature of this cryptographic setup is based on ensuring that the computational cost of hacking such a system far outruns the possible gains that could be made. The processing power required to circumvent this cryptography extends far beyond the reaches of the largest multinational corporations such as Google or Microsoft and are therefore well outside the reaches of basement hackers. The technique used is known as a “proof-of-work” based system which can only be resolved through brute force application of computing power. This power is normally used by swarms of miners through pools of distributed processors over large periods of time resulting in the sharing of the discovered Bitcoins. This ensures that the effort of the miners is rewarded and no single entity is capable of exploiting the system to unfairly gain Bitcoins.
A Brief history of Bitcoin

Before Bitcoin, various attempts had been made towards introducing a feasible digital currency. The key task of these early innovators was based around ascribing value to their new currency. The earliest of these online currencies were based around the gold standard and came in market after the IT-bubble had burst in the late 1990s.

Companies such as OS-Gold, Standard Reserve and INTGold came to existence between 1999 and 2004. But they didn’t last very long due to their externalised dependency on necessary reserves that needed to be held as gold. However the people running these companies diverted the deposited funds leading to several million dollars worth of loss for the account holders.

Other companies such as e-gold and e-Bullion also faced investigation by the United States government with legal disputes still ongoing. Due to enforcement by US government agencies these companies had their assets frozen and seized leading to the discovery of criminal acts as well as fraud. Although not all cases have resulted in clear violation of law, it has effectively placed gold based digital currency in shutdown.

Another form of digital currency that caught the public interest prior to 2001 was Beenz. com’s online currency called beenz. It was earned by individuals when they performed certain online activities and was then used as e-currency for purchasing services online. The marketing campaign was very successful and garnered nearly USD 100 million from venture capitalists from the international market. However, the legality of operating an independent currency led to numerous conflicts with many nations across America and Europe.

Charges of operating an unlicensed bank plagued the company but were soon resolved. At its peak Beenz operated in 12 countries including US, Japan, China and Australia. The company couldn’t survive as a currency due to its dependence on banks and airline points systems which suffered in post 9/11 America. The currency was integrated into their customer relationship management tool and phased out slowly.
The first significant name in true cryptographic digital currency came with DigiCash which was founded far before all others in 1990 but declared bankruptcy in 1998 and was sold off to Ecash. David Chaum’s Ecash was also an anonymous e-cash system secured by RSA signatures. By 2002 the company running the system failed again and was sold off to another company disappearing from public existence.

The only other digital currencies that found footing in the international market existed in virtual economies or synthetic economies. These economies emerged out of a continuously ongoing virtual world where the exchange of goods took place within the context of a networked game. These massively multiplayer online role playing games (MMORPGs) created virtual worlds that connected millions of people who were the foundation of the economy. Players could use the currency of the virtual economies in these games to purchase virtual goods for use in the game. As time and engagement took over, players were able to leverage the virtual products against real world value and make real economic gains.

Life simulation games like Second Life also created virtual economies that made it easier to link virtual and real economic transactions using in-game currency convertibility. The Linden Dollars from Second Life are used to pay for assets created in the game as reward of intellectual property via in-world content creation and trade. This currency was able to trade for real world goods and currency via third party sites. Conversely, other online games like World of Warcraft, Warhammer and Final Fantasy XI became controversial settings where real money was used to make in-game purchases between players. Game companies attempted to dissuade this by reinforcing in-game currency to be convertible.

All these centralised and loosely based virtual currencies remained highly marginalised by their natural drawbacks until a cryptographic decentralised digital currency system was created - this was Bitcoin. The conceptual idea behind Bitcoin was introduced by a mysterious figure using the pseudonym Satoshi Nakamoto in a paper - Bitcoin: A Peer-to-Peer Electronic Cash System - in November 2008. The paper outlined the logic method of attaining an electronic transaction protocol that could eliminate issues of trust. The first active Bitcoin network went live in January 2009 and was accessed using the first version of the open source Bitcoin client.

The first block of 50 BTC was mined by Satoshi Nakamoto. Over a period of months various vulnerabilities were discovered and patched resulting
in the rectification of 184 million fraudulent Bitcoins. Since then no new vulnerabilities have been discovered in the protocol.

As the proliferation of the Bitcoin client, protocol and awareness of its system gained wider reach it began to garner a loyal following with various parties using it for payments online. Websites such as WikiLeaks started using it as a valid medium for donations as well as secure anonymous payments across the world. Bitcoin garnered lots of negative attention due to its use in the Silk Road - an online black market - as it became the currency of choice for darknet transactions involving various illegal trades and activities including drugs and hitmen.

Various legitimate online communities and business’ such as Reddit, Wordpress, Pirate Bay and nearly a thousand others have begun accepting Bitcoins as payment or donations. The faith of the online community in the use of Bitcoins is highly encouraging towards its promise as a future standard for digital currency.

Various nations have dealt with the Bitcoin phenomenon in different ways. The United States has closely monitored the evolution and use of Bitcoins but beyond the individual level. Their concern has primarily been with respect to how it is used in money laundering activities by criminals as well as the monitoring the role of private companies or groups in transacting real money which is in contradiction with financial laws.

Countries like China and Thailand have aggressively discouraged the use of Bitcoins due to the lack of legal frameworks that govern it. Countries such as Germany have even begun considering Bitcoins as a valid form of e-currency due to its exhibited properties as a unit of account but not as a normal currency in real world use. But the bulk of the force behind Bitcoin comes from its users and merchants, with recent revelations in Bitcoin insurance by Lloyds of London and acceptance by mainstream online companies like Overstock and Zynga.

**Bitcoin as currency**

Bitcoins is the name given to the units of money or currency used on the Bitcoin protocol. Its abbreviation is “BTC” i.e. 1 BTC, like 1 USD for United States Dollar. Unlike analogue currency Bitcoins do not exist in physical form, rather only as numbers associated with a Bitcoin address that identify their value. This number can be replicated in physical tokens such as physical coins, paper print outs or card like objects but are only identifiable as genuine currency on the Bitcoin peer-to-peer distributed network by the
This form of currency coding, unlike serial numbers on paper currency, is highly secure due to its unique identification on the Bitcoin registry that validates the coin instantly for online transfers.

Bitcoins are created on the Bitcoin network through the act of “mining” which we cover in greater detail in subsequent chapters. However, the term “mining” refers to the act of discovering Bitcoins through applied effort (computational) on the Bitcoin network similar to the act of mining for gold or other precious commodities. The computational effort taken by “miners” on the network is reflected by the solving of complex mathematical problems which requires brute force processing power and therefore is an investment of time and energy.

The mathematical problem is a “proof of work” solution that result in the awarding of Bitcoins to the miner and the creation of new blocks. The difficulty of these problems can vary based on the strength of the network as well as the proportionate reward of Bitcoins. The network is based on an open source peer distributed software that has rigid parameters that govern the payoff. The system is designed to be easier during the start of the process, resulting in larger payoffs, and reduces by half every four years that the Bitcoin network is active. So a solution in 2010 would have yielded twice as many Bitcoins as it does in 2014 and will yield half as many Bitcoins in 2018 and so on.

The system is designed on a transparent mathematical system that can be predicted to create a finite number of Bitcoins in its running time. The approximate number of Bitcoins generated in the first four years of operations or 210,000 blocks, from January 2009 to November 2012 was 10,499,889.80231183 and will result in half as many more by December 2016. By this count the currency supply will gradually and incrementally keep increasing until it hits a fixed ceiling beyond which more Bitcoins
won’t be created irrespective of mining efforts. The total number of Bitcoins that can ever be in existence are just less than 21 million at around 20,999,839.77085749 when using the determined 8 decimal point.

The system is designed to reveal blocks every 10 minutes with the initial value of 50 Bitcoins per block. Along with the runtime reduction in Bitcoin payoff, another aspect of the system is that it adaptively changes the difficulty of the mining process based on the rate at which processing power is dedicated to the task. This adaptive reiteration takes place every 2016 blocks based on the time taken to solve that many blocks.

At the current time (January 2014) there are 12274575 BTC in existence with a steady rate of increase. The number of Bitcoins in existence can be easily checked at [http://blockexplorer.com/q/totalbc]. And as the network runtime increases the number of Bitcoins mined will half to 12.5 after the next 210,000 blocks and then 6.25 and so on. Due to this iterative division Bitcoins are divisible down to 8 decimal places. Similar to analogue currency, Bitcoins are also used in smaller denominations. The smallest denomination is .00000001 BTC but can be even lower if the existing protocol is augmented.

Similar to paisa or cents, Bitcoins are used in fractions of centiBitcoin (bitcent = .01 BTC), milliBitcoin (mbit = .001 BTC) and microBitcoin (ubit = .000001 BTC). Due to the international nature of the digital currency, Bitcoin denominations are named within the metric SI system rather than imperial or colloquial units such as cents, pence or pound. The only exception is the honorific given to the smallest unit i.e. .00000001 BTC which is called a satoshi. It is named after the pseudonymous creator of the Bitcoin protocol Satoshi Nakamoto.

![Diagram of a Bitcoin](image-url)
IntroductIon to BITcoIn

Bitcoin as a decentralised digital currency

Many users of digital currencies, specially Bitcoin, express concerns relating to it being a fraudulent scheme designed to fool people into exchanging real currency for alpha-numeric sequences that have no actual value. But as we have observed value is generated through community trust in the system of the currency itself. The use of Bitcoins within the system doesn't assure any participant unfair gains or profits. The currency benefits from its decentralised nature which ensures that no individual or institution is at the core of it and positioned to unfairly benefit from its use.

The Bitcoin system is based on early low reward efforts leading to long term community benefits. The first persons to mine for Bitcoins were not at a significant advantage as the value of Bitcoins at the time was negligible or close to 10,000 BTC for a pizza (we don't know which one). At todays rates just 1 BTC would easily purchase 100 pizzas. But for the system to be functional in the early days the Bitcoins needed to be used in transactions that didn't value the Bitcoins very highly - a reflection of its nascent trustworthiness.

There was no government or agency that could artificially increase the value of the Bitcoin due to its decentralised nature. The value had to evolve from continuous usage and proliferation of the user network both in the digital as well as real world. Bitcoins are now accepted in over one thousand locations across the world including real world locations such as cafes and restaurants.

Another unique aspect of this decentralised nature is that unlike other fiat currencies, Bitcoin isn't an inflationary currency with its value being
dwindled by increasing supply, however it is the reverse. Bitcoin is predicted to experience deflationary forces over time due to its pre-determinedly limited supply. As Bitcoins are lost due to technical issues, accidents or seizure (government) the value of the Bitcoin will more rapidly stabilize and find a normal level. However, there is also the possibility that with occasional and continuous losses due to random events, the supply of Bitcoins in circulation with always remain significantly lower than the total supply created. And unlike normal currency this deflation will effect the laws of supply and demand in unpredictable ways. The likely outcome is that the value of Bitcoins will increase as scarcity will relatively increase over time which will in effect cause aberrant trading behaviour causing Bitcoin value to fluctuate.

In order to resist this possibility the system is designed for infinite divisibility of unit. In practice, while at one point 10,000 BTC could buy a pizza, today only a fraction of one Bitcoin is needed. By continuously being able to engage a lower unit of Bitcoin, a centicoin or an ucoin for trading the problem of deflation could also be managed. By dividing the Bitcoins to its lower denominations indefinitely usage could evolve in a practical and manageable way within the decentralised system.

**Foundations of Bitcoin’s Value**

Bitcoins in most physical forms contain an inscribed motto - Vires in Numeris - latin for “Strength in Numbers”. The philosophy and design of the
Bitcoin protocol is based on this saying and uses it to uphold the system within which Bitcoins function.

For any currency to have usefulness they need to have value, which in the case of Bitcoins comes from its scarcity. The system ensures a limit on the number of Bitcoins and scarcity in its production. As the community of Bitcoin users moves to further adopt the currency and the number of users increase, so does the strength of the currency. The faith placed by the first adopters, the miners who worked to generate the currency, Bitcoins are a unit of trust. Their trust and subsequently the trust of all users is in the mathematical perfection of the system that allows users the comfort of knowing that their Bitcoins are unique, valuable and represent value.

Similar to the older Gold Standard, which was supposed to allow currencies to be redeemed for gold as backing, Bitcoins are based on the premise that people within the network - retailers, merchants and individuals - will continue to accept them and trade value will be retained.

At its very core Bitcoins are based in trust and faith in the currency itself, which is similar to most modern fiat currencies with the exception of an institutional or governmental support. The faith usually given to central banks and governments is given to the purity of the code that runs Bitcoin in ensuring that it remains secure and safe in the digital wallets of the users. The value of the Bitcoin also can’t be controlled or manipulated by governments as is the case with fiat currencies and the effects of inflation are negligible in the long run since the supply of the currency can’t be increased. Bitcoin’s value is solely in the hands of its users and based on the foundational laws of supply and demand, clear of any external manipulations.

This raw dependency on market forces and lack of any correctional or protectionist third party (government) is considered by many as both a blessing as well as a curse. Since the trading of Bitcoins takes place across digital platforms there is a rapid and global influence from a large number of users reacting to a vast variety of reasons such as rumours, fear, confidence issues, local laws and other behavioural factors. These variations in motivations, without corrective measures in place, makes the value of Bitcoins fluctuate rapidly, causing further fears of it being nothing more than a bubble. However, this phenomenon isn’t untrue for fiat currencies as history has shown. Bubbles are common in free market currencies such as the dollar and euro but they are always seen to normalise in the long run, which is the expectation from Bitcoin as well.
Is Bitcoin a revolution?

Bitcoin is the youngest currency in the world. It is also the world’s first and fastest emerging currency of trust. Pure mathematical certainty. And that trust is what makes Bitcoin a force to be reckoned with more than any of its other features. It represents not only security and efficiency but also a dynamic form of democracy.

And even though it is based on a man-made open source software system, the system can’t be changed without majority approval from those who make up the system. This distribution and decentralisation give Bitcoin its greatest strengths as they free participants from having to trust each other or a central agency. They just have to trust the math. Faced with numerous large scale financial meltdown over the last 20 years, it isn’t unusual for people to seek certainty when it comes to their money. After watching governments plunder, waste and inefficiently use national currencies, the idea of a digital currency free from the flawed clutches of government are a source of peace.

This peace is a form of liberty that many Bitcoiners embrace with great passion and conviction. By taking the control out of governments and private agencies, individuals are able to not only reduce costs of currency transactions (as compared to other forms of online transactions) but also increase the value of the currency over decentralised currency exchanges. The currency attains value as a unit of exchange as well as a speculative investment that can grow. All without having to pay governments any form of tax, fees or other share of profits. And if libertarian philosophy doesn’t motivate people to participate, then surely denying the government any share of profits is incentive enough for a revolution.

The Bitcoin revolution looks more like a rollercoaster when we look at how its users work with it.
In order to spend Bitcoins you need to have some and getting your hands on a few can be quite the task, we take you through the process and let you know the easiest way to go about it.
The time is ripe to mine Bitcoins! While the statement would’ve been more accurate had it been said two years ago, it still is a good time to start mining. Now if you don’t understand what mining is then the most simple way to put it would be that it is one of the ways of obtaining Bitcoins and its variants i.e. Litecoins and Dogecoins. Anyone with a computer can mine Bitcoins, the process is that simple. You only need a client and you have to let it run continuously for a while till you start generating coins. Or so we may think, but little did you know that with each waking moment the Bitcoin mining process keeps on becoming incrementally more difficult. So the more time you take to get in on the action the lesser of a profit you’ll be able to make.

**Bitcoin generation**

Basically, you are crunching an awful lot of numbers to get Bitcoins as a reward in return. But since it is digital you’ll need some mechanism so that people just don’t copy a set of bitcoins and then try to spend it all over again. Afterall, double spending is a characteristic of digital currency. This is where the whole proof-of-work function comes into the picture. Bitcoin uses the hashcash proof-of-work function as the backbone of its mining algorithm. Every mining software that is working endlessly is trying to create a proof-of-work which makes their work unique and thus entitles them to a set of coins. Bitcoin uses an algorithm called hashcash to generate proof-of-work. It is costly in terms of time and energy consumed to produce for the pre-defined parameters. But at the same time it shouldn’t require as much time to verify a proof-of-work as it takes to produce it. This is why the entire process revolves around scanning for a value that when it is hashed two times with the SHA-256 hashing algorithm, the resulting hash begins with a pre-defined number of zero bits. The average effort needed to hash such numbers increases exponentially with an increase in the number of zero bits required. This same generated hash however, can be easily verified by rehashing the number with a single pass of the double SHA-256 algorithm. So it is easy to verify but difficult to generate.

Then a simple question arises, if it was difficult to create for one machine then maybe two can do the job better. This is undoubtedly true, adding more hardware to the mix will give you more bitcoins but only for a short while. When you increase the number of zero bits you increase the difficulty. And the Bitcoin network has its difficulty parameter readjusted every two weeks so that as time passes and more powerful computers join the
network, the rate of creation is kept static. So the more popular it gets, the harder it becomes to generate bitcoins. So much that normal computers can no longer generate bitcoins at a profit. The amount spent for the electricity will far outweigh the value of the generated bitcoins. Yet people continue to mine. This is because of the specialised hardware that has been released which can generate bitcoins at a pace far greater than ever before but while consuming far lesser amount of electricity..

Whenever anyone generates a proof-of-work it becomes part of the blockchain. The blockchain then serves as a ledger for every transaction that ever takes place. This is why all your transactions in the Bitcoin ecosystem can be traced from the very origin. Only after verification is the bitcoin transaction happen. So if anyone would’ve programmed a bitcoin wallet to show a balance of bitcoins that never existed it couldn’t ever be used. This is called the double spending problem and the concept of bitcoin was conceived in order to solve the double spending problem. Whenever digital currency is generated, there is the possibility of copying that currency. And thus creating a duplicate which can be used like the original currency. Bitcoin does not have this issue thanks to the blockchain. Any person trying to scam the system needs to rewrite a good portion of the blockchain and that can only be done via a consensus. That is, a majority of the clients hosting the blockchain must be convinced that a new addition/modification is infact been seen by a majority of the clients. Unless this happens the new addition/modification is rejected. So it would take a few of the world’s fastest supercomputers to actually change the balance of the bitcoin economy. All of this makes the Bitcoin system very difficult to scam.

Glossary

Usually reserved for the end, it would be advisable to go through the glossary now itself to get a better understanding of things to follow.

**Bitcoins** - It is a cryptocurrency that is generated and used within the bitcoin ecosystem. The currency is very volatile and the current value is roughly around USD 900.

**Block** - Blocks are individual links in a chain of transaction verifications. Transactions that are outstanding get added into a block and are verified approximately every ten minutes. Each new block generated helps with the verification of all previous blocks since it adds upon the previous one. Data is permanently recorded in the Bitcoin distributed network through files called blocks.
Block Chain - Each block that is generated has the hash of the previous block included in it. This creates a link to every coin ever mined in the bitcoin network. When a lot of such blocks come together you get a blockchain. A block chain can also considered as a history of transactions which is shared by all nodes that are mining or participating in the Bitcoin ecosystem or basically a digital ledger. A complete copy of the bitcoin blockchain of a will have every movement of every coin ever mined.

Difficulty - About every 2016 blocks that are released, the Bitcoin ecosystem adjusts the difficulty of verifying blocks depending upon the time taken for the previous 2016 blocks. This is roughly considered to be an increment of 20-30% of the previous value. The difficulty parameter is adjusted so as to keep the average bitcoin generation rate static and only one block will verified on an average of ten minutes for the next 2016 blocks. This “difficulty” parameter is usually expressed as a number [the difficulty at the time of writing this article was 1,789,546,951]. The difficulty is designed to be inversely proportional to the target.

Double-Spending - Trying to spend bitcoins or any digital currency that has already been spent in a previous transaction

Generate Bitcoins - When a miner finally finds a block, it gets virgin bitcoins as a reward. The number of bitcoins awarded for verifying a new block is 25 BTC for each segment of 210,000 blocks. It used to be 50 BTC per block but this number goes down every subsequent 210,000 blocks or so. It has been 4 years since the inception of bitcoins when the first 210,000 blocks were verified and since the rate of generation is constant, it will be another 4 years before the number of BTC awarded is halved again. The total amount of bitcoins that will ever be mined has been calculated to be approximately 21 million BTC.

Hash - The output generated by a hash function is called a hash.

Hash function - It is a computer algorithm which takes any input data and then runs it through a few calculations and shifting processes before generating a fixed length output called the hash. Passwords are commonly stored as a hash so that your actual password is never stored anywhere. Depending on the algorithm used, the probability of two inputs having the same hash does exist. In the Bitcoin system, a hash is difficult to produce but easy to verify and forms the backbone of the whole mining process.

Hash rate - The number of hashes calculated by the hardware is the hash rate. Commonly used indices are Megahashes/second and Giga-hashes/second.
Miner - It is a computer software or a hardware that is designed to calculate the hashes needed for the inception of a new block. The miner also gets a reward in the form of bitcoins and transaction fees for aiding in the creation and the maintenance of the bitcoin blockchain.

Node - Every participant is a node in the bitcoin network, certain client allow you to save a copy of the blockchain on your computer while some don’t. Nevertheless, they are both nodes.

Satoshi - The smallest unit of a Bitcoin which amounts to 0.00000001 BTC is called a Satoshi after the creator of Bitcoin i.e., Satoshi Nakamoto.

Transaction Fee - This is a fee that is added voluntarily to any transaction so as to add the transaction to the block. The fee also determines whether a transaction will be added or not since a higher transaction fee gains priority over lower transaction fee. Since it is voluntary it may be added with any transaction but it is the sender who always pays the fee since bitcoin transactions are always one sided. For transactions that are large which means a high addition needs to be done to the blockchain a fee is expected and charged by most online services.

Virgin bitcoin - When a miner generates a block that has never been spent a Virgin bitcoin is produced as a reward. Thus it is the only true anonymous portion of the bitcoin system. All subsequent transactions can be traced back to the virgin bitcoin.

Mining
Anybody can mine bitcoins, there is a lot of material available online which can guide you through your choice of hardware and software. We’ve gone through some of them to curate all the methods and the time taken to generate bitcoins with each of them. First, we will look at the different hardware that is available in the market for mining bitcoins.

There are different types of hardware available in the market. You can use your ordinary computer [or your super-awesome-rig, whatever you call it] to mine or you can purchase specialised hardware made for mining and nothing else. The hash calculation process is very simple but the sheer volume of calculations is quite taxing on the system. We have four popular options on a broad scale. Along with each hardware type will be a chart detailing different models of each hardware available in the market and the hash rate it offers in MHash/second(higher is better).

1. CPU
2. GPU
3. FPGA
4. ASIC
**CPU**

The CPU is simply the Central Processing Unit or your computer’s processor. This is the easiest and the most commonly obtainable hardware. Also it would be prudent to mention that you don’t need to go and get a separate processor at this moment. The problem with using your CPU is that it isn’t designed for the volume of calculations involved. You will be able to mine coins in the long run but the costs associated with it will be astronomical and in no way will you be able to break even. The only place where CPU based mining becomes feasible is for criminals who have botnets that mine Bitcoins on all infected computers and according to a recent report, India ranks 4th in the number of PCs having malware mining Bitcoins.

**GPU**

The Graphics Processing Unit is the processor that sits in the heart of your graphics card or more recently on your main CPU itself in the form on on-chip GPU. GPUs are more focussed towards mining since they have a reduced instruction set compared to CPUs. CPUs are designed to calculate a wide variety of instructions hence the focus is more on compatibility and less on volume. GPUs on the other hand have a much reduced instruction set in comparison and can crunch out a lot of numbers in a short amount of time.

<table>
<thead>
<tr>
<th>Model</th>
<th>Mhash/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pentium M1.6ghz</td>
<td>0.4</td>
</tr>
<tr>
<td>Pentium M1.6ghz</td>
<td>0.71</td>
</tr>
<tr>
<td>Pentium Dual-Core E2180</td>
<td>4.5</td>
</tr>
<tr>
<td>Pentium Dual-Core E5400</td>
<td>2.27</td>
</tr>
<tr>
<td>Core 2 Quad Q6600</td>
<td>11</td>
</tr>
<tr>
<td>Core 2 Quad Q9650</td>
<td>18.67</td>
</tr>
<tr>
<td>Core i3-2100</td>
<td>8.28</td>
</tr>
<tr>
<td>Core i5 2500K</td>
<td>20.6</td>
</tr>
<tr>
<td>Core i5 2600K</td>
<td>17.3</td>
</tr>
<tr>
<td>Core i7 2600K</td>
<td>18.6</td>
</tr>
<tr>
<td>Core i7 980x</td>
<td>19.2</td>
</tr>
<tr>
<td>Core i7 990x</td>
<td>33.3</td>
</tr>
<tr>
<td>Core i7 3770k</td>
<td>5.2</td>
</tr>
<tr>
<td>Core i7 3930k</td>
<td>66.6</td>
</tr>
<tr>
<td>Xeon W3680</td>
<td>18</td>
</tr>
<tr>
<td>Atom N450</td>
<td>1.6</td>
</tr>
<tr>
<td>Atom N550</td>
<td>1.97</td>
</tr>
<tr>
<td>Atom D510</td>
<td>2.3</td>
</tr>
<tr>
<td>4x Opteron 6174</td>
<td>115</td>
</tr>
<tr>
<td>Athlon XP 2000+</td>
<td>0.62</td>
</tr>
<tr>
<td>Opteron 8220 x16</td>
<td>25</td>
</tr>
<tr>
<td>Phenom II X4 965</td>
<td>12</td>
</tr>
<tr>
<td>Phenom II X6 1055T</td>
<td>23.6</td>
</tr>
<tr>
<td>Phenom II X6 1075T</td>
<td>21.3</td>
</tr>
<tr>
<td>Phenom II X6 1100T</td>
<td>22</td>
</tr>
<tr>
<td>Turion X2 RM-70</td>
<td>1.9</td>
</tr>
<tr>
<td>A4-3400</td>
<td>23.2</td>
</tr>
<tr>
<td>A8-3850</td>
<td>60</td>
</tr>
<tr>
<td>A8-3870K</td>
<td>95</td>
</tr>
<tr>
<td>A10-5800K</td>
<td>105</td>
</tr>
<tr>
<td>NVIDIA</td>
<td>Model</td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
</tr>
<tr>
<td>ION</td>
<td>1.8</td>
</tr>
<tr>
<td>8600GT</td>
<td>5.66</td>
</tr>
<tr>
<td>8800GT</td>
<td>34</td>
</tr>
<tr>
<td>9600GT</td>
<td>15.66</td>
</tr>
<tr>
<td>9800GT</td>
<td>30.36</td>
</tr>
<tr>
<td>G210</td>
<td>3.38</td>
</tr>
<tr>
<td>GTX260</td>
<td>44</td>
</tr>
<tr>
<td>GTX275</td>
<td>58</td>
</tr>
<tr>
<td>GTX295</td>
<td>117.3</td>
</tr>
<tr>
<td>GT 325M</td>
<td>7.5</td>
</tr>
<tr>
<td>GT440</td>
<td>20.4</td>
</tr>
<tr>
<td>GT530</td>
<td>17.9</td>
</tr>
<tr>
<td>GTX460</td>
<td>66.32</td>
</tr>
<tr>
<td>GTX480</td>
<td>140.43</td>
</tr>
<tr>
<td>GTX560 Ti</td>
<td>100</td>
</tr>
<tr>
<td>GTX570</td>
<td>160</td>
</tr>
<tr>
<td>GTX580</td>
<td>156.6</td>
</tr>
<tr>
<td>GTX590</td>
<td>193.1</td>
</tr>
<tr>
<td>GTX670</td>
<td>112</td>
</tr>
<tr>
<td>GTX680</td>
<td>120</td>
</tr>
<tr>
<td>Quadro FX 770M</td>
<td>6.39</td>
</tr>
<tr>
<td>Quadro FX 880M</td>
<td>9.6</td>
</tr>
<tr>
<td>Quadro FX 1600M</td>
<td>6</td>
</tr>
<tr>
<td>Quadro FX 1800</td>
<td>13.6</td>
</tr>
<tr>
<td>Quadro NVS 3100M</td>
<td>3.6</td>
</tr>
<tr>
<td>Quadro NVS 4200M</td>
<td>10</td>
</tr>
<tr>
<td>Quadro 5000</td>
<td>67.7</td>
</tr>
<tr>
<td>Tesla K20</td>
<td>134.8</td>
</tr>
<tr>
<td>Tesla M2050</td>
<td>94.5</td>
</tr>
<tr>
<td>Tesla S1070</td>
<td>155.2</td>
</tr>
<tr>
<td>Tesla S2070</td>
<td>749.23</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AMD</th>
<th>Model</th>
<th>Mhash/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>5850</td>
<td>240.77</td>
<td></td>
</tr>
<tr>
<td>5850x6</td>
<td>2,135</td>
<td></td>
</tr>
<tr>
<td>5870M</td>
<td>152.5</td>
<td></td>
</tr>
<tr>
<td>5970</td>
<td>863.4</td>
<td></td>
</tr>
<tr>
<td>6310M</td>
<td>9.821</td>
<td></td>
</tr>
<tr>
<td>6450</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>6570</td>
<td>114</td>
<td></td>
</tr>
<tr>
<td>6770</td>
<td>235</td>
<td></td>
</tr>
<tr>
<td>6850</td>
<td>301.4</td>
<td></td>
</tr>
<tr>
<td>6870</td>
<td>339.25</td>
<td></td>
</tr>
<tr>
<td>6950</td>
<td>454.4</td>
<td></td>
</tr>
<tr>
<td>6970</td>
<td>433</td>
<td></td>
</tr>
<tr>
<td>6990</td>
<td>865</td>
<td></td>
</tr>
<tr>
<td>6990x2</td>
<td>1436</td>
<td></td>
</tr>
<tr>
<td>6990x3</td>
<td>2094</td>
<td></td>
</tr>
<tr>
<td>7750</td>
<td>104.15</td>
<td></td>
</tr>
<tr>
<td>7790</td>
<td>313</td>
<td></td>
</tr>
<tr>
<td>7850</td>
<td>363</td>
<td></td>
</tr>
<tr>
<td>7870</td>
<td>460</td>
<td></td>
</tr>
<tr>
<td>7950</td>
<td>605</td>
<td></td>
</tr>
<tr>
<td>7970</td>
<td>710</td>
<td></td>
</tr>
<tr>
<td>7970x3</td>
<td>1950</td>
<td></td>
</tr>
<tr>
<td>FirePro V3800</td>
<td>69</td>
<td></td>
</tr>
<tr>
<td>FirePro V4800</td>
<td>79.7</td>
<td></td>
</tr>
<tr>
<td>FirePro V8700</td>
<td>84.8</td>
<td></td>
</tr>
<tr>
<td>FirePro M5800</td>
<td>61.4</td>
<td></td>
</tr>
<tr>
<td>FirePro M5950</td>
<td>96.7</td>
<td></td>
</tr>
<tr>
<td>FirePro V7750</td>
<td>35.7</td>
<td></td>
</tr>
<tr>
<td>FirePro V7800</td>
<td>254.85</td>
<td></td>
</tr>
<tr>
<td>FirePro M7820</td>
<td>150</td>
<td></td>
</tr>
</tbody>
</table>

Needless to say, AMD cards are way better than NVIDIA’s offerings and this is because of the architecture they have. AMD’s GPUs have many simple shaders that run at low clock frequency while the NVIDIA design has a lot lesser CUDA cores which run at a relatively higher frequency. So AMD gets
the upper hand by having way more parallel processing throughput, when we compare the AMD 6990 to the NVIDIA 590 we can see that:

- AMD Radeon HD 6990: 3072 ALUs x 830 MHz = 2550 billion 32-bit instruction per second
- Nvidia GTX 590: 1024 ALUs x 1214 MHz = 1243 billion 32-bit instruction per second

Right off these numbers we can see that AMD is ahead by twice the margin. Another factor is how the instruction sets are implemented in the two competing devices. AMD's instruction set is capable of doing what NVIDIA's instruction set does in 1/2 number of steps. This significant advantage in terms of time combined with the sheer raw output puts AMD ahead of NVIDIA.

**FPGA**

A Field Programmable Gate Array is a chip that comes as a blank slate. You can mount the chip and then program it to do whatever you want to get done. This is the reason why the “Field Programmable” part of the name exists. Now these are fabricated according to order as the number of logic gates on each chip can be customised. Also, there are a lot of FPGA packages available for cheap, you can simply purchase them in bulk and start programming each chip to mine bitcoins. They are also quite cheap, but since the design isn’t streamlined, it isn’t as fast as the ASIC but it is way faster than a CPU and comparable to a GPU.

We can see that the Mini Rig by Butterfly Labs is as good as an ASIC miner even though it is FPGA. And most of the FPGA are comparable to GPUs.

**ASIC**

Application-Specific Integrated Circuit” are basically designed from the ground up to do just one particular task. They are absolutely useless
These are the fastest sort of mining hardware at the moment. There are some manufacturers like Avalon, ASIC-Miner, Butterfly Labs etc, who have released hardware based on ASIC chips which are highly evolved for bitcoin mining.

For a little comparison on which hardware is better you can check the following link: [https://en.bitcoin.it/wiki/Mining_hardware_comparison](https://en.bitcoin.it/wiki/Mining_hardware_comparison)

### Pick your coin

There are a lot of alternatives in the Cryptocurrency universe. Bitcoins have become ridiculously difficult to mine and only ASIC machines are actually worth the effort. Other currencies, however, are catching up. You do have

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>MHash/S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avalon ASIC #1</td>
<td>66,300</td>
</tr>
<tr>
<td>Avalon ASIC #2</td>
<td>82,000</td>
</tr>
<tr>
<td>Axon Synapse Terra-1</td>
<td>3,000,000</td>
</tr>
<tr>
<td>BitForce SC 5Gh/s</td>
<td>5,000</td>
</tr>
<tr>
<td>BitForce SC 10 Gh/s</td>
<td>10,000</td>
</tr>
<tr>
<td>BitForce SC 25 Gh/s</td>
<td>25,000</td>
</tr>
<tr>
<td>BitForce Little Single</td>
<td>30,000</td>
</tr>
<tr>
<td>BitForce SC 50 Gh/s</td>
<td>50,000</td>
</tr>
<tr>
<td>BitForce Single ‘SC’</td>
<td>60,000</td>
</tr>
<tr>
<td>250 GH/s Rack Mount Bitcoin Miner</td>
<td>250,000</td>
</tr>
<tr>
<td>BitForce 500 GH/s Mini Rig SC</td>
<td>500,000</td>
</tr>
<tr>
<td>BitFury’s</td>
<td>120,000</td>
</tr>
<tr>
<td>Bitmine.ch Avalon Clone 85GH</td>
<td>85,000</td>
</tr>
<tr>
<td>Black Arrow Prospero X-1</td>
<td>64,000</td>
</tr>
<tr>
<td>Black Arrow Prospero X-3</td>
<td>1,344,000</td>
</tr>
<tr>
<td>Blue Fury</td>
<td>2,500</td>
</tr>
<tr>
<td>Block Erupter Blade</td>
<td>10,752</td>
</tr>
<tr>
<td>Block Erupter Cube</td>
<td>30,000</td>
</tr>
<tr>
<td>Block Erupter Emerald</td>
<td>336</td>
</tr>
<tr>
<td>Block Erupter Sapphire</td>
<td>333</td>
</tr>
<tr>
<td>CoinTerra TerraMiner IV</td>
<td>2,000,000</td>
</tr>
<tr>
<td>HashBlaster “I” – 20nm</td>
<td>3,300,000</td>
</tr>
<tr>
<td>HashFast Baby Jet – First Batch Backorder</td>
<td>400,000</td>
</tr>
<tr>
<td>HashFast Baby Jet – Second Batch</td>
<td>400,000</td>
</tr>
<tr>
<td>HashFast Sierra - Second Batch</td>
<td>1,200,000</td>
</tr>
<tr>
<td>KnCMiner Mercury</td>
<td>100,000</td>
</tr>
<tr>
<td>KnC Saturn</td>
<td>250,000</td>
</tr>
<tr>
<td>KnC Jupiter</td>
<td>500,000</td>
</tr>
<tr>
<td>KnC Neptune</td>
<td>3,000,000</td>
</tr>
<tr>
<td>Monarch BPU 300 C</td>
<td>300,000</td>
</tr>
<tr>
<td>Monarch BPU 600 C</td>
<td>600,000</td>
</tr>
<tr>
<td>TerraHash Klondike 16</td>
<td>4,500</td>
</tr>
<tr>
<td>TerraHash Klondike 64</td>
<td>18,000</td>
</tr>
<tr>
<td>TerraHash DX Mini (full)</td>
<td>90,000</td>
</tr>
<tr>
<td>TerraHash DX Large (full)</td>
<td>180,000</td>
</tr>
<tr>
<td>Xtreme Miners Leopard 2.5 Th</td>
<td>2,500,000</td>
</tr>
<tr>
<td>Xtreme Miners Tiger 5 Th</td>
<td>5,000,000</td>
</tr>
<tr>
<td>Xtreme Miners Lion 7.5 Th</td>
<td>7,500,000</td>
</tr>
</tbody>
</table>
Litecoin and Dogecoin which are currently the popular alternatives to Bitcoin. They do not in any way have the same returns but consider these coins to be in their infancy. If you do get in on the action now then hopefully in the next 4 years you could possibly be a multi-millionaire. The current exchange rate stands as follows.

- Litecoin - 1,500 Rupees/coin
- Dogecoin - 5 Paise/coin

Litecoin is relatively difficult to mine than Dogecoins but it has already started gaining traction so that makes it a viable investment.

**Solo / Pool / Rental**

Mining is by no means an easy task. In the next few paragraphs you will come to know how difficult mining solo is so why don’t we look at some numbers.

Let’s say you have a good rig which can handle three AMD HD 7970 cards in CrossFire configuration. Each card gives an estimated 700 MHash/s but the CrossFire configuration will give you 1950 MHash/s on an average. The electricity cost per kWh in India is roughly 20 paise / kWh when generated. Consumer rates are even higher and vary from place to place. The current Bitcoin generation difficulty is at 1,789,546,951. Under these conditions we can calculate the rate of generation.

| **Coins per 24h at these conditions** | 0.0005 BTC |
| **Power cost per 24h** | 0.01 USD |
| **Revenue per day** | 0.44 USD |
| **Less power costs** | 0.43 USD |
| **System efficiency** | 19.50 MH/s/W |
| **Mining Factor 100 at the end of the time frame** | 0.02 USD/24h@100MHash/s |
| **Average Mining Factor 100** | 0.02 USD/24h@100MHash/s |
| **Power cost per time frame** | 0.66 USD |
| **Revenue per time frame** | 37.56 USD |
| **Less power costs** | 36.90 USD |

As you can see, with such a configuration that has three GPUs totalling Rs. One Lakh you only end up with 0.01 USD per day after subtracting electricity costs. This is ridiculously depressing for someone who spent close to a lakh for purely mining these coins. If you aren’t part of a pool then your profitability goes down even further since you will only generate one block every 124 years. That’s right, more than a century is needed and
that is why solo mining is only for those who have a supercomputer(s) at their disposal.

Pool mining is another aspect where you do have the same rig but there are a lot many folk just like you who come together to form the pool. This pool then cumulatively works to solve one block and thus the success rate is much higher and increases as the number of participants in the pool goes up. While this also means that the share that each user gets is way low, it does guarantee to certain extent that you will mine some bitcoins out of the venture rather than solo mining wherein uncertainty looms over you for 124 years.

The last option is to rent processing power. Imagine that there are people who can get you the hardware resources but don't have the money to fund themselves. They turn to consumers and start offering rental services. In this method, you pay to get a certain processing power. They do everything for you so that all you need to worry about is getting your money’s worth in time. That is the problem with upcoming hardware and services. There isn’t any guarantee and some only accept payment in Bitcoins, so there is no way of getting your money back. Butterfly labs is one company that has delivered on their promises and are now seeking customers to buy into the rental business. They charge USD 10.53 / [GHash/s]. So if you do spend the same amount as for the triple crossfire AMD setup then you pay close to USD 2,499. Let’s run the calculation again now.

<table>
<thead>
<tr>
<th>Coins per 24h at these conditions</th>
<th>0.0667 BTC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power cost per 24h</td>
<td>0.01 USD</td>
</tr>
<tr>
<td>Revenue per day</td>
<td>53.22 USD</td>
</tr>
<tr>
<td>Less power costs</td>
<td>53.21 USD</td>
</tr>
<tr>
<td>System efficiency</td>
<td>2373.20 MH/s/W</td>
</tr>
<tr>
<td>Mining Factor 100 at the end of the time frame</td>
<td>0.02 USD/24h@100MHash/s</td>
</tr>
<tr>
<td>Average Mining Factor 100</td>
<td>0.02 USD/24h@100MHash/s</td>
</tr>
<tr>
<td>Power cost per time frame</td>
<td>0.66 USD</td>
</tr>
<tr>
<td>Revenue per time frame</td>
<td>4571.41 USD</td>
</tr>
<tr>
<td>Less power costs</td>
<td>4570.75 USD</td>
</tr>
</tbody>
</table>

Now power costs are irrelevant since you are not paying for that and all you are investing is for the processing power. This means that in just 49 days you will mint enough bitcoins to break even. Everything after that is pure profit. The rental agreement lasts for one year so that means USD
16,817 of profit over a year. Seems too good to be true? Well, these calculations are based on the current difficulty rate and as time goes by this will increase and you will find it more difficult to mine. That means that the returns reduce significantly. Moreover, they haven’t started the service yet which means by the time they do open their doors to the general public the profitability goes down even further. Since there is no clear release timeline at the moment we can’t calculate the estimate for breaking even your initial investment.

There are plenty of tools available online to help you get estimates on your hardware. Check out http://www.bitcoinx.com/profit/ for a well thought out calculator.

**Software for mining**
The hardware is just one part of bitcoin mining. You need to worry about the software as well. There are quite a few software but we’ll mention the more popular ones that are widely supported.

1. BFG
2. BitMiner
3. BTCMiner
4. cgminer
5. Diablo
6. EasyMiner
7. gMinor
8. GroupFabric
9. MPBM
10. Phoenix
11. poclbm

Not all of them support GPUs and ASIC and lastly, FPGA mining. One that does all three is cgminer, however, it may be a bit difficult for beginners to fiddle with since there is a fair bit of tweaking involved in getting it to work. We don’t know if you’ve noticed but the GPU lists in the previous section did not feature recent GPUs, that is because the high end GPUs have undergone a slight architectural change and it will be a short while before these software start working on those GPUs.

If you are going to be using ASIC or FPGA then you need to figure out which software out of these is supported by your hardware. As for those you wish to mine on their computers, cgminer should be more than sufficient.

**Join a pool**
If the numbers weren’t convincing enough then we’re letting you know that solo mining is as good as dead. You need to join a pool in order to actually get something out of all the effort you’re going to be putting in. There
are plenty of pools out there but you need to join up in a pool with a lot of participants. The following four have the highest number of participants and the highest output.

- Slush’s pool (mining.bitcoin.cz)
- BTC Guild
- Eligius
- GHash.IO

When you register an ID at each pool, you will be given a worker ID and PASSWORD. For each worker [i.e. individual machine] you need to create a new worker ID and PASSWORD. If you own 5 ASIC machines then 5 IDs and PASSWORDS will be needed, one for each. You can join multiple pools as well and then gather different worker IDs and PASSWORDs from each pool.

**cgminer Example**

Let’s say you’ve finally got the hardware together and are ready to mine a few bitcoins. We’ll walk you through a simple cgminer command line. At each pool you’ll get a pool URL and a PORT. Aside from that you need to get the following ready.

- Hardware [GPUs/FPGA/ASIC]
- Appropriate drivers installed
- For GPUs you need to install the OpenCL package from the respective manufacturer
  AMD


If your cgminer windows looks like this once you run the command then you’ve got it right!
NVIDIA
https://developer.nvidia.com/opencl

- Have cgminer installed
  Command line:
  For mining in a single pool all you need to do is use the following command line and replace the pool:port with the url given to you and the username and password with the appropriate worker ID and PASSWORD.
  
  cgminer -o http://pool:port -u username -p password

  For multiple pools you need to chain the commands one after the other and create a huge command with all URLs, worker IDs and PASSWORDs.

  Multiple pools:

  Press enter and if all goes well, you should start mining and see something like the image on the previous page.

  There are a lot more clients and covering each and every usage scenario for all of them wouldn’t be possible so it would be best to join an online Bitcoin community and find out if others with your same hardware have found a convenient software to use.

  That’s about it for generating bitcoins. Once you’ve started on this you need to figure out how to use that currency. The next two chapters focus on usage of bitcoins and other cryptocurrencies.
TRADING BITCOINS

This new crypto-currency doesn’t adhere to the normal system that we have in place. Here is how it works.

We don’t really have to say that something which appreciated in value by approximately 850% over the last six months is one of the best investments you can get into. However, the valuation of Bitcoins has gone up and down like a roller coaster ride over the same period. Very similar to a stock market this commodity has had severe ups and downs with the worst in recent times being a drop of 61% If you wish to picture that in your mind then think of Wiley E. Coyote falling off a cliff. And just like the fantastic Mr. Coyote even
Bitcoins have risen just as easily. Bitcoins gained immense publicity last year which was the most well performing year for the currency. Billionaires have arisen and disappeared with the inventor of the cryptocurrency being the first billionaire having a net worth of $1.1Billion. Unfortunately, he isn't featured on the Forbes list since he is only a billionaire each time the bitcoin exchange rate touches $1000. Also, there is the likely possibility that this person doesn’t exist since the name Satoshi Nakamoto has been hailed as pseudonym.

**So why is it a good investment?**

There are multiple factors to something being a good investment, while we aren’t investment gurus it isn’t rocket science to figure out what could possibly be a good thing to invest in. Let’s take a look at the facts, this is a cryptocurrency that has been around for slightly over 4 years now and in this period it has grown immensely. So it’s a well performing concept. The number of coins that can be mined is limited to 21 million coins. So there is never going to be a dilution as is the case with stocks. In fact the parameter of difficulty which we went into in the last chapter ensures that the mining process is maintained at a constant pace till all 21 million coins are in circulation. Also since the quantity is limited the rate per Bitcoin is only going to go up. This makes it similar to ever natural resource we have on earth which happens to be limited and thus gains value over time. The final aspect that adds value to something is acceptance; and Bitcoin has been well received over the years. Online retailers have started accepting Bitcoins, donation services have started accepting Bitcoins. Even the Singapore government is currently planning to tax Bitcoins so even official channels have opened up

![BTC > USD exchange rate over one year (2013)](image-url)
and finally Bitcoin ATMs are now being rolled out. What more of a justification could one need to deem Bitcoins as worthy of investment.

**The situation in India**

While mining and trading has been going on for quite some time and that too at a level similar to what most countries have, the prospect of exchanging Bitcoins into real world cash has been more or less difficult. Ever since the whole hullabaloo over black money, trading is somewhat risky as it does put traders under the scrutiny of the authorities. There wouldn’t be anything wrong with it but reports of Bitcoins being used for funding the cause of anti-social elements has led to some inconvenience. The recent notice by the RBI [can be read here](http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247) has led to a lot of Indian Bitcoin exchanges shutting shop or temporarily suspending services. Few of the said services have restarted their services but the uncertainty of trusting a new player in the market always exists.

**Going about it all**

Now that the gloomy, boring and rather discouraging part about trading is over, let’s get into the thick of the whole trading business. Before you start with anything you’d want someplace to store your Bitcoins. While real world currency has a whole centralised system in place the digital currency is more decentralised.

**Wallet**

The first step is to get a wallet for yourself. The wallet is from where you send and receive Bitcoins. There are multiple websites and software that allow you to set up a wallet. But you need to remember that with all the crackdown on various services a third party system could go down any day and with that all your Bitcoins will disappear. That’s a worst case scenario but something that has been happening. There are three types of wallets you can go with.

1. **Software based**

   These are software that you download onto your system and let’s you start immediately. There are plenty of software avail-
able with Bitcoin-Qt, MultiBit, Armory and Electrum being the most popular ones.

2. Mobile wallets
Adding an extra layer of flexibility gives you the option of carrying your Bitcoin wallet around with you on your smartphone. Most of these clients are free and some of them link up to your NFC so you can pay using the same at stores that accept Bitcoins.

3. Web-service
If you don’t want to worry about hosting your precious Bitcoins on your personal computer or mobile device then you have the option of web-services where all you need to do is make an account.

Reliability
The whole centralised aspect of Bitcoins brings a debilitating effect to it and that is reliability. The wallet is the one place where your Bitcoins stay, there is no backup unless you make one. Real world has banks that offer insurance but none of the applications you download or the web-services you opt for gives you any guarantee. Quite simply because they can't, while the transactions can be tracked easily the identity of the person owning the account cannot be unless they choose to. So that being said, the software based clients hosted on your machines are the safest. You can make plenty of backups and sync them whenever you make a transaction. The probability of losing all backups simultaneously is pretty low.

Mobile apps are similarly reliable but certain apps were removed from their respective stores [Coinbase was removed from the App store] so that’s there. This doesn’t mean loss of Bitcoins but those who’d downloaded it could still use it. Also losing your mobile phone meant you’d lose your Bitcoins to some lucky pickpocket.

Websites can go down at any moment and should be used as an intermediary if you care about privacy. Hosting your Bitcoins solely on a web-service is the least recommended option.
Recap: How transactions work
If you didn’t pay attention the last time then you’ve gotten another chance at understanding the Bitcoin transaction.

Let’s say you want to purchase some product with Bitcoins. When you surf the product page you will be given a QR code to scan. The reason a QR code is given is that the addresses to which you have to send are rather long and have jumbled letters so the possibility of entering the wrong address is very much there. This is why the entire process has been simplified with the use of QR codes. Once you scan the QR code into your wallet software, the QR code is analysed to give you the address and cost of the item along with the label column where you can see the particulars of the transaction. If you’re into shady transactions then all you will see is the address and the amount, labels are optional.

Once you hit “send” in your client, the details are patched to the nearest node of the Bitcoin network, this is then multicast till the address to which you want to send the money is located. This may take a ridiculous amount of time depending on where the receiving address is and what kind of network it is situated in. High-privacy networks like Tor take a much longer time for transactions to reach their final destination.

Moreover, there is often a transaction fee which the sender has to pay for which is minimal. All transactions can be easily tracked in the Bitcoin ecosystem. Each Bitcoin that has ever been generated can be tracked right down to the current owner. Which is why scamming the system is very difficult but scamming people is quite easy. The decimal trick is the easiest, Bitcoin transactions take place in numbers that have 8 decimals. So by shifting the decimal point scamsters make quite the buck, so all clients now have
an exchange index which shows the actual value in dollars at the moment so any foul play with the decimal pops up instantly.

**Anatomy of a wallet**

Once you’ve downloaded a wallet software there will be a few new elements since this is a new concept. All wallet services will have a few essential things common with the rest being added features. For the purpose of explaining the workings of the system we’ll be using the most simple wallet we could find – Multibit.

Download the software from [https://multibit.org/](https://multibit.org/) and install it. When you start the client you will be shown the welcome screen as is below.

The interface is fairly easy to comprehend. The top left corner shows your balance across all wallets. Yes, you can have multiple wallets in one software and in this particular software you can see all your wallets on the left. Adding wallets is as easy as clicking the “New Wallet” button beneath that panel.

On the top right hand corner you can see the current exchange rate for BTC > USD which is at 916 dollars/BTC. This can be customised and we’ll show you how. In the centre we have the tabs for sending, receiving and for

![Multibit home-screen](https://thinkdigit.com)
monitoring all transactions done through this software. In order to customise your exchange rate ticker open up the “Preferences” panel.

Scroll down till you find the “Currency ticker and Exchange rate” section. Tick the check box to show the second row. Select “OpenExchangeRates” under exchange. Then click on “Get App ID”. You’ll be taken to the OpenExchangeRate website where you’ll need to create a free account. Once done you’ll get an APP ID which will be a bunch of alphanumeric characters. Copy the app ID and paste it in the Multibit client under the “OpenExchangeRates App ID” column. Then select INR from the Currency menu in the second row. Apply the settings and you’ll soon see the exchange rate for BTC > INR on the top row. It was Rs.52,240 at the time of writing this article.

Receiving bitcoins
Your wallet is setup and now you can start off with your Bitcoin wallet. All you need are some Bitcoins. But first you’ll need some coins. You can either mine the coins as explained in the previous chapter or you could go to any exchange and purchase the Bitcoins. Once you do that you’ll need to transfer those Bitcoins to your wallet and for that you’ll need to use the receive tab. Here you need to put down the label and the amount. Both these
columns are optional but it’s good for book-keeping anyway. Once you do that you’ll see the QR code on the right has changed and all you need to do is send this QR code to whomsoever needs to pay you. Once they scan the QR code in a wallet application they will see your address [the long alphanumeric set of letters], the amount and the label. Then can then choose to send the same amount or different amount to the address. Once done you’ll see your BTC balance adjust to show the amount credited to your wallet. It is advised to use a new address each time you make a transaction. In this example, we’ve generated a QR code for transferring 1 BTC and we’ll be using the same in the next example.

**Sending Bitcoins**

Now that you have a few Bitcoins in your wallet you can start making purchases. Open the send tab and here you’ll find a column to enter the address to which the money is to be sent and below that you’ll see the label and the amount to be sent. If you’ve been given a QR code then simply paste that into the box on the right and all the details pertaining to the transaction should pop up. If you have enough balance in your wallet then by all means press send and complete the transaction.
Securing your wallet
Your wallet is the only thing that has all the information about your Bitcoins so keeping that safe is of the utmost importance. So here are a few simple things to keep in mind.

1. Check and recheck
The decimal point trick is pretty easy to catch but scamsters have much better ways of parting you from your Bitcoins which is why all transactions must be double checked before you go through them.

2. Multiple wallets
Have one main wallet and a lot of mini wallets for each payment option. This way nobody ever gets to know about your main wallet since all payments and receipts are channelled via smaller wallets. Another good thing about this practise is that if at all you do lose some Bitcoins it will be one of your smaller wallets and not your main one.

3. Backup
Each wallet service/client employs some method to backup your funds. Some
of them only backup a certain portion of the wallet which means when they are recovered you might not get your complete balance back. This is part of the privacy feature that certain clients have, so they only backup those transactions which are labelled as public. Another common feature that most web services now offer is the ability to sync your wallet with Dropbox or similar services. This way your wallet is synchronised after every transaction. It would be wise to have more than one backup service attached to your account. Finally, you should encrypt your wallet which is also offered by many services. MtGox doesn’t allow you to buy or sell without attaching a security service to your account. Google’s Authenticator is widely supported so you can have two step authentication with each wallet. Finally, having a CD/DVD/USB flash drive is also recommended for regular backups. We do understand how tedious the entire process becomes when you have a multitude of backups to take after each transaction but it’s all in your favour.

4. **Multisignature**

At its core the Bitcoin protocol makes use of two keys – a public key and a private key. When you need to make transactions these keys come into play. Now the Bitcoin protocol allows for more than one person’s digital keys to be required for each transaction. Think of it like a joint bank account where more than one person has to sign the cheque. So you can choose if a minimum of 2 or 3 signatories are needed per transaction.

5. **Hardware wallets**

These should be the epitome of security but they don’t exist at the moment. They are designed to be a wallet and do nothing else, since that makes it a single purpose entity, the chances of breaking the system is minimal.

6. **Succession**

Wallets can easily be entrusted to others and if you forget your password then the other person might be able to remember it. This also helps if under any circumstances the owner were to be no longer able to operate the wallet then a successor could take over. Memorising the password has always been a good strategy but in this case forgetting the password gives you no means to recover the wallet.

**Anonymity**

Bitcoin is not anonymous. We’ve mentioned this before that every single
transaction ever performed since the generation of a coin can be traced back. So as long as you have an address, you can see every single transaction that was directed to or originated from that address. Which is why we mentioned that each address should only be used for one transaction to ensure security. The identity of the owner to whom the address belongs to is kept a secret unless you’ve made transactions that reveal your identity. In that case all transaction you will ever perform can be tracked. Certain clients like Bitcoin-Qt gives you the ability to create two return addresses so that does help a bit, but it can still be traced back if necessary.

Still need anonymity?
Enter Zerocoin, it is a proposed extension to the Bitcoin protocol which means implementation of the Zerocoin system shouldn’t be difficult at all. Zerocoin includes a system to launder Bitcoins in the blockchain itself so that tracing a transaction becomes next to impossible giving you true privacy. The concept is just a research paper at the moment and is being worked on, hopefully we should see demonstrations happening in late 2014. Essentially, when your Bitcoins enter the system there are a few Zerocoins which are generated and your Bitcoins are converted into Zerocoins which then get transacted here and there before finally being spent. At the end of the blockchain you get your coins back but the entire process that happened in the middle makes the transaction anonymous.

However, if you are still worried about getting a bit of privacy then you can opt for a laundry service which takes transactions from many users, breaks it down to a lot more micro-transactions and then shuffles them between the users before finally bringing it together and returning it to the user. The catch
Trading bitcoins is that all these transactions are stored in the blockchain and the difficulty of tracing is increased only if there are a lot of users in the laundry service. Unfortunately, most services don't enjoy that kind of volume of users.

**Bitcoin Exchanges**

An exchange is where real world cash can be used to trade in Bitcoins. So you don’t need to mine Bitcoins on your own you can simply buy a few coins and then start using the Bitcoin system to make payments. There are several exchanges and there are Indian Bitcoin exchanges too. However, we strongly advise against using any service that isn’t registered with the authorities. Mt.Gox is the most popular Bitcoin exchange there is and we’ll walk you through the process of getting a few coins.

You’ll need to create an account first which includes sending a government issues proof of identity and proof of residence. Without these two you will not be able to buy or sell Bitcoins at Mt.Gox. The documents are only accessible to staff members of Mt.Gox so you don’t need to worry about it getting into the hands of anyone else. Do note that you will not be able to use a Credit card or any similar reversible method for purchasing Bitcoins since Bitcoin transactions are irreversible. You’ll have to use Direct deposit or a service like Moneygram. Until you verify your account you won’t be able to transfer money to your Mt.Gox account and you’ll see the following image.

![Add Funds Withdraw Funds Redeem Codes](image)

A government issued ID proof is needed to operate some exchange accounts.
However, if you do have a redeemable code from Mt.Gox given to you by someone then you can use it without any need for verification. All transactions are processed manually so they take an awful amount of time to transfer money to and fro.

**Indian websites**

If you wish to obtain coins in India without the hassle of getting your money converted into dollars first then check out [https://localbitcoins.com/country/IN](https://localbitcoins.com/country/IN). There will be a few registered users who volunteer to act as an intermediary. Also there is a reputation system in place which only allows trusted people to buy/sell Bitcoins. However, a reputation system is easily scammed using multiple accounts so that is one thing you need to worry about. But in this website they’ve included an escrow service. So you are going to be transferring your money to the website and not to the trader. The trader in return transfers Bitcoins to the website. Once the website detects that both parties have upheld their end of the deal it releases the payment to the respective parties. Also the company behind the website is registered with the authorities in Finland so that should allay any fears of being a shady website.

---

**Arbitrage trading**

The exchange rates at different Bitcoin exchanges are different. So naturally we have arbitrage trading happening. In case you are wondering what that means, arbitrage trading involves in trading Bitcoins for real cash at one exchange and then using the cash for buying Bitcoins at a cheaper rate than the first exchange. The only downside is that the transactions take an awful long time to happen at most websites and you might miss out on deals giving the waiting time.

Now that you’ve read in on how to trade Bitcoins, you might want to figure out a way to start offering Bitcoins as a method of payment on your website. That’s what the next chapter is about. 

---

*Arbitrage is about buying low and selling high*
It’s only prudent that you incorporate this multibillion dollar medium of payment into your business.

Now that Bitcoin is gaining popularity the time has come to start considering Bitcoins as a mode of payment system for e-commerce. Also since the value of Bitcoin has only gone up since its inception makes it a worthy investment. The current ecosystem is well developed and easily linked to bank accounts while Bitcoins follow an entirely different system altogether. We’ve found some
payment gateways that have already been established and a few innovative ways to monetise content.

**The hard way**
If you don’t have a large volume of sales and wish to experiment with Bitcoins as a currency then you can do so manually which we’ve explained in the previous chapter. All you need to do is to create a wallet once you’ve downloaded a client. Then generate the address and amount you wish to sell a product for [do check the exchange rate when you calculate the amount]. Once the QR code is generated using the above details, simply give the customer the QR code by displaying it on a screen in your establishment. The customer can simply scan the code and pay for the goods. As volume increases, manually generating codes becomes cumbersome and you have to resort to an automated process. This is where payment processors come into the picture.

**Payment Gateway**
If volatility of the Bitcoin exchange rate is a cause for concern then you need not worry since these payment gateways allow you to set prices in your local currency which is then converted into Bitcoins at the moment of purchase.
so you’ll get an equivalent amount of Bitcoins. Here are some of the more popular payment gateways.

1. Mt.Gox
There are quite a few payment gateways you can use without worrying about losing your finds. Mt.Gox has its own API for accepting payment straight into your Mt.Gox account. It doesn’t matter whether the consumer has a Mt.Gox account or not, even if they have a wallet then the store page will show the QR code once you’ve confirmed the order. So you can use any wallet software to pay. The Mt.Gox API can be found on their website along with the documentation on how to make use of it. Depending on what language your website was built on you can choose a plugin accordingly. For more information check the following link [https://en.bitcoin.it/wiki/MtGox/API/HTTP/v1]

2. Coinbase
Coinbase is another popular gateway with merchant services included. Which means they provide a wallet to store your Bitcoins which you can convert to real cash when you please.

3. BIPS
BIPS offers a complete merchant solution and has features like mobile checkout, point of sale system, currency conversion etc. Moreover, you can use any of the pre-existing plugins to enable Bitcoin payments on any of the countless open source e-commerce website CMS. Wordpress, woocommerce, magneto, zencart, wp e-commerce, opencart etc., are some of the commonly used CMS and they are all supported by BIPS.

4. BitPay
This is a slightly older service since it has been around for some time. Like the previous payment processors, even BitPay offers plugins for all the popular e-commerce CMS.

5. Coinkite
With offerings of hardware this POS is more catered to physical stores. They have their own billing system along with the Coinkite cards which can be used as normal debit cards. Though they haven’t released their system it does look promising. But what if the card system doesn’t catch around, you can
still use the QR code which the Coinkite terminal comes with built-in. You can generate and scan QR codes using the terminal making it a replacement in entirety. Check a demonstration video here [http://vimeo.com/82032338].

**Taxes**

If you accept cash at your store then you do have to pay taxes for the same. Cash is just as anonymous as Bitcoins. If there is a system in place then Bitcoins should be taxable too. But India does not have a system in place at the moment to handle the Bitcoin ecosystem and hence there are no taxes at the moment. However, we are not affiliated with the Tax department in any way so we can’t be sure. If Bitcoins do turn out to be popular then by all means the government will find out a way of going about the system and taxing it. However, with more anonymous forms of Cryptocurrency on the horizon this should be a difficult task.

**Methods**

There are three ways of implementing Bitcoin payments on your website.

**Method 1. Use an API**

There are plenty of services out there that allow you to implement their code on your website. You are given the API documentation and may have to create an account on the website. Once an account is created you will be given a wallet or an API ID. This ID will then be used in the website code to generate “calls” to the API. The service then returns a QR code or the latest exchange rate or whatever you were after. Since there is a usage of third party resource in this scenario you might stick to a trusted provider. On top of that, since the hardware of the service provider is being used they might charge a small transaction fee. Some services have a simple subscription program while others may subtract a percentage of your transaction.

Here is a simple PHP script by BIPS

```php
$ch = curl_init();
curl_setopt_array($ch, array(?CURLOPT_URL => 'https://bips.me/api/v1/invoice',
```
• CURLOPT
• T_USERPWD => 'apikey',
• CURLOPT_POSTFIELDS =>
  'price=100&currency=USD&item=TEST&custom='.
  json_encode(array('o
• rder_id' => '1', 'returnurl' =>
  rawurlencode('http://domain.com'))),
• CURLOPT_RETURNTRANSFER => true,
• CURLOPT_HTTPAUTH => CURLAUTH_BASIC));
• $url = curl_exec($ch);
• curl_close($ch);
• header('Location:
  ' .
  $url
  );

Under T_USERPWD - you will enter the API key generated when you create an account in their website. This API key is simply a Bitcoin address where the money will go to.

Under price - you can modify the entry to reflect the price or simple refer to a variable which hosts the price of the object being sold.

Once you implement the code with all the relevant details you should be able make calls to the BIPS server from where the QR code will be generated and sent to your website for rendering.

Free alternative
You could skip that step and have your own QR code generated by a free service like Wolfram Alpha and use the return value on your page.

Example.
http://www.wolframalpha.com/input/?i=bitcoin%3A1NYsMtFgaSWvcTg4sM5fRGSZTcZeSkXsYM%3Famount%3D0.01%26%3Blabel%3DTimepass+qr+code
Enter the address after bitcoin% , in this case it is 3A1NYsMtFgaSWvcTg4sM5fRGSZTcZeSkXsYM
Enter the amount after amount%3D in bitcoins, in this case it is 0.01 BTC
Enter the label after label%3D , in this case it is Timepass

Method 2: Use a plugin
Needless to say, this is the easier alternative. You can get plugins for any
of the countless e-commerce CMS from most payment processors. You do have to fiddle with the configuration to get it working, especially if you have a version mismatch or are on an older CMS while the plugin is for a relatively new version of the CMS. Almost all the services we’ve mentioned before offer plugins for the popular CMS out there. If your CMS isn’t that popular then you can take the plugin for the CMS that yours was derived from and tweak it a bit to suit your CMS.

Method 3: Embedded solutions
This is pretty much the same as the previous method except there is no need for any tinkering here. There are plenty of such packages wherein the Bitcoin payment processor is embedded into the CMS so as soon as you deploy it you are ready to accept payments. We’ve mentioned some of them here but they are all paid services so there is a price to pay for the convenience.

Shopify - A subscription service where everything is hosted on their servers. You just need a warehouse to get started.
3Dcart - A similar subscription based service for e-commerce websites.
E-GovLink - Aimed towards enabling local governments to accept payments for utility services and so forth.

**For all you bloggers and entrepreneurs**

A lot of people have blogs and there are websites that curate content from multiple bloggers and host it on their website. A neat way to monetise the content is to start charging a subscription fee. This is where Bitmonet helps you out. With Bitmonet you can just give a preview or a summary or a certain article. The moment someone is interested and wants to read it they have to pay up. So Bitmonet’s plugin allows you to create vouchers or “passes” as they call it. You can have a single article pass, a day pass or even monthly subscriptions. For the service they charge a small amount in terms of a transaction fee paid by the reader. They even have a demo page on their website to help you get a better understanding of what it does. [http://bitmonet.com/](http://bitmonet.com/) Moreover, it has a plugin for Wordpress and there is a code generator for Blogger and Tumblr so you can monetise that too.

Now, if you are an app developer then you can add Bitcoin as a payment method to your apps as well. In collaboration with Coinbase the folks behind Bitmoney have come up with a SDK to add the ability to accept Bitcoins in android. [http://bitmonet.com/blog/demo-video-monetize-you-android-app-with-bitcoins/](http://bitmonet.com/blog/demo-video-monetize-you-android-app-with-bitcoins/)

That was all that you needed to do in order to start receiving bitcoins via your e-commerce shop, blog, app or even your neighbourhood retail store.
ALTERNATIVES TO BITCOINS

Ever since Bitcoin hit the scene nearly 70 other cryptocurrencies have gone into circulation. We take a look at the biggest ones.

Bitcoin isn’t the only player on the digital currency playing field. With many imitators and successors already active in the online world the future of digital currencies looks to be safeguarded. We take a look at some of the altcoins that may be serious contenders.

Ripple

Ripple was created as an open source payment protocol for online transactions by Ryan Fugger. It’s being developed by Ripple Labs with significant investment from sources such as Google Ventures. The Ripple network
also falls under the distributed peer-to-peer transaction model but is also useful in currency exchanges, with current support for numerous currencies. It is the second largest cryptocurrency with USD$ 2,036,364,833 market capitalisation.

The network maintains a publicly shared database that records all transactions and currency activity. Its decision making system is based on community consensus and takes up to 5 seconds to clear a transaction. Beyond its role as a transaction network Ripple also works with its own currency internally known as “ripples” or XRP. It’s not a mandatory part of the network and treats all currencies alike for trading and transactional purposes.

Ripple is quickly catching up to Bitcoin in usage and may be the next generation of virtual currency protocols.

Ripple is made up of “gateways” that represent merchants willing to accept deposits from users which is then reflected as the holdings of users on the Ripple network. Unlike Bitcoin or Litecoin or any of the other digital currencies, Ripple does not rely on its currency as much as it does on its network protocol which is very similar to how normal banks operate. Except that the network of transaction is public as compared to a private setup by individual banks. All deposits and transactions are in public record which can be redeemed from “gateways” for fiat currencies. The system has an element of risk like those in normal banks where a bank can default on deposits made, similarly so can a gateway. The strength of the system is believed to
be a more efficient and secure online transaction method that works within traditional financial systems at a lower transaction cost to users.

**Litecoin**

Litecoin is the third largest open source digital peer-to-peer cryptocurrency in the world based on the market capitalisation of USD $586,759,042. It is built on the Bitcoin protocol - designed to be decentralised and has no central operator. The goal of its design is to upgrade some features that are thought to be lacking in the Bitcoin system and presents itself as a viable alternative to Bitcoin. Just like Bitcoin it is divisible to 100,000,000 units with LTC as its signifier.

The main differences from Bitcoin include faster transaction confirmations. As we know the Bitcoin protocol takes 10 minutes to process a block which needs to be confirmed in the ledger. Litecoin processes blocks every 2.5 minutes allowing for faster confirmations. This also increases the networks security against attacks for double spending. Litecoin is also based on a different proof-of-work system using scrypt. This key difference is a means to deny miners with GPU, FPGA and ASIC systems an advantage over regular CPU owners. Normally it is harder for ASIC and FPGA systems to work with scrypt making the process of mining using these hardware is more expensive. However this claim is under debate with evidence indicating that the result is in fact the opposite due to its poor use of scrypt.

The goal behind the intended difficulty is to ensure that a select group of individuals who can afford high end computing power do not unfairly gains most of the Litecoins that are mined. This system is intended to make small scale miners achieve a level playing field.

The Litecoin system is designed to produce just under 84 million litecoins and it was valued at USD $592,061,706 on January 8th 2014.

**Peercoin**

Unlike Bitcoin or Litecoin, which are cryptocurrencies based on a proof-of-work implementation, Peercoin or PPC uses a hybrid proof-of-stake and proof-of-work system. It uses the same source code as Bitcoin for its network design and is currently the 4th largest cryptocurrency (market cap of USD$ 120,985,892). The system doesn’t limit the number of coins that can be generated but ensures a one percent annual rate of inflation. Along with this feature, the mining process is considered more energy efficient which makes it scalable in the long term period.
The purpose of the proof-of-stake inclusion in its systems is meant to protect the currency from dangers that Bitcoin faces i.e. that if 51% of mining share is under a single control mechanism the currency can be manipulated (double spending) which would collapse the value of the currency. Since as mining rewards decrease with Bitcoin over time, there is a real possibility that mining will become highly monopolised allowing the possibility for a 51% attack. By having a hybrid system, new coin production is related to the how many coins are held by individuals i.e. someone with 1 percent of the Peercoins will create 1 percent of all proof-of-stake blocks. With an unlimited coin supply this will ensure that the cost of attempting a monopoly is a sufficient disincentive. Initially the system is built using proof-of-work implementation which gradually transitions to proof-of-stake as the former’s difficulty increases.

**Mastercoin**

Mastercoin is one of the strangest cryptocurrency systems in use today. Mastercoin is positioned as the fifth largest currency with a market capitalisation of USD$ 59,901,198 and interestingly the highest dollar exchange value next to Bitcoin.

Based on the Bitcoin protocol and not the currency model, Mastercoin is meant to “be used as a protocol layer, on top of which new currency layers with new rules can be built without changing the foundation”, according to the developer J. R. Willett in his whitepaper - “The Second Bitcoin Whitepaper”. It uses the already active Bitcoin protocol in order to create its own currency.

Mastercoin does not run on its own network or create new blocks or invite miners to dedicate power to earn coins. Instead its focused on creating new networks of currencies, commodities and securities using the Bitcoin protocol that is already in place. It uses the Bitcoin blockchain to store all its transactions and allows users with a host of new features such as the ability to create their own currency on the Mastercoin network.

The network functions as a decentralised exchange that negotiates between any two currencies by carrying orders for currencies on the Bitcoin blockchain and pairing it on the peer-to-peer network with a suitable pair instantly, without involvement from the offering party. Simply put, an individual could decide to sell 10 BTC at the rate of 1000 LTC for every 1 BTC and the offer is matched by someone else on the network by Mastercoin who is willing to make the exchange at that price.
Mastercoin also uses the protocol to work as price feeds that can update and inform users of prices of various goods and commodities through the scripts. Along with these commercially finance features, Mastercoin is also able register speculative trades or bets between people based on the value of the coin itself in a “price spread” style which allows financial hedging and arbitrage with lower levels of currency risk and volatility.

**Primecoin**
Primecoin is created by the same person as Peercoin, Sunny King, who employs a different proof-of-work system for this cryptocurrency. Primecoin is based on the same principles as Bitcoin except its mining efforts are based on searches for chains of prime numbers. Using this cryptographic technique disallows GPUs from participating in mining efforts.

The key variations from Bitcoin are that the computational efforts invested for Bitcoin’s hashcash proof-of-work system do not provide any other value beyond the creation of Bitcoins. With Primecoin’s system of prime search proof-of-work the combined computational power of mining results in the discovery of long Cunningham chains of prime numbers that are of significant interest to the academic and scientific community. Already this system has resulted in the discovery of long Cunningham chains.

Another benefit of Primecoin is its faster block creation time which is 1 new block per minute as compared to Bitcoin’s 1 new block every 10 minutes. Due to this faster block creation, the resulting Primecoin transactions are also 10 times as fast however the difficulty on the Primecoin protocol is adjusted with everyblock as compared to Bitcoin’s 2016 blocks. Along
with this, the number of Primecoins awarded per block is also variable, in a positive correlation with the difficulty of the block.

Primecoin is the 12th largest cryptocurrency in the world with a market capitalisation of USD $13,122,112 and 4,059,356 units as of January 2014.

**Namecoin**

Namecoin is hybrid cryptocurrency that functions more than just a currency. It is created with the ability to be an alternative and decentralised DNS that seeks to protect domain names from censorship and take them out of the control of ICANN. It does this by creating a new top level domain outside ICANN.

Namecoin is the sixth largest cryptocurrency in the world (market cap = USD$ 45,209,707) and uses a slightly modified version of the Bitcoin protocol. It is also restricted to 21 million units with 123,616 .bit domains being registered. Instead of awarding traditional “coins”, Namecoin awards .bit domains which are used as currency.

**Dogecoin**

Dogecoin is the 13th largest cryptocurrency in the world as has a market cap of USD$ 12,154,567. Its upper limit of production is at 100 bullion units of which 28% have been mined. It is also the most recent addition to cryptocurrencies, having launched on 6 December 2013. It has seen remarkable growth since then, both in terms of interest from miners as
well as appreciation of value. Despite its rocky start with attacks on its wallet systems by hackers Dogecoin trading has been higher than all other currencies combined (including Bitcoin). Its design is based on the Litecoin system and uses scrypt in its proof-of-work algorithm.

**Laxmicoin**

The list of altcoins wouldn’t be complete without India’s inclusion in the foray. Laxmicoin is the proposed name for a digital currency that is yet to be launched. It is being organised and coordinated by developers from Bangalore who are currently negotiating its validity with Indian regulators in the Reserve Bank of India. Their website - laxmicoin.com - is currently only accepting email id which will be update when the site becomes active and intermittently active on twitter and Facebook.

The currency is expected to be based either solely on the Bitcoin protocol or the Ripple protocol with discussions still ongoing within and outside the developer group. The question remains whether it will simply copy an already established protocol system like Bitcoin or Ripple, or will it introduce something new that will make it more relevant to the Indian context where internet and computer penetration is low, as well as higher costs of mining exist. Its promoters can easily be contacted online for further information.
As the rest of the world deals with the impact of the rise of digital currencies, India is not far behind. We take a look at the equation of Bitcoin with India.

Over the past couple of years the potential of Bitcoin as a virtual currency as well as a trading security have attracted many Indians - both business’ and individuals. The Indian Bitcoin community is estimated to be anywhere between 30,000 to 50,000 people strong and growing. As more and more people begin taking part in this new economy the government has also taken interest and started
engaging the community. We will take a look at the current state of the Bitcoin phenomenon in India as well as its potential.

**Bitcoin Conference**

The level of interest over Bitcoin in India reached such high levels that a Bitcoin Conference was organised where active parties and curious individuals could gather. Titled as - The Global Bitcoin Conference - it was organised in Bangalore by CoinMonk Ventures. The conference was divided into two days - first for socialising and the second for panel discussions where 20 speakers from various backgrounds discussed Bitcoin and its various aspects.

In addition to the panel discussion the conference also had participant booths that promoted and educated attendees about various new products and technologies related to Bitcoin. The booths ranged from CoinMonk’s own booth that sold gold coins with the Bitcoin symbol on it, as well as selling physical Bitcoins. They also demonstrated how Bitcoin mining takes place.

The other booths present dealt with three key areas of Bitcoin - mining, trading and alternatives. The areas on trading included presentations by BTC Robot and BitcoineX.in that are automated trading tools and Bitcoin exchanges respectively. In addition to which there were informative booths that talked about Laxmicoin the highly anticipated Indian version of Bitcoin that was expected to be launched soon.

The panels were divided into four key areas of discussion - Bitcoin and decentralisation, mining and security, Bitcoin trading, and Bitcoin regulations, trends and altcoins. The discussions placed various individuals from specialised fields together to present their viewpoints on the issues. The conference brought together bankers, technologists, cryptographers and business’ as they presented their arguments in favor of Bitcoin for the Indian audience.

This conference was definitely one sided which isn’t uncommon for a gathering of this type - privately organised, agenda driven and meant to convert as many people to the cause as possible. The main promises made were based around the immense potential Bitcoin has towards personal profit making. This point in specific is very much against the intended purpose of the Bitcoin philosophy. As a currency Bitcoin is intended to free people from extra costs and make transactions more convenient and trustworthy, however by advocating for short-term profit in trading, it is unlikely that the currency would find an easy acceptance in the broader marketplace. Speculative trading on Bitcoins, which is what was significantly highlighted at the conference, weakens the overall potential of Bitcoin finding stability
Bitcoins in India is already on the rise with a limited reach but in a diverse distribution.

in exchanges and having any worthwhile future as a mainstream currency. As a venue for learning more about Bitcoins, this conference gave a thorough introduction to the elementary concepts of Bitcoin mining and usage. However the talks given about its feasibility from a financial point of view were lacking in depth and painted a slightly oversimplified image, specially within the Indian context. The majority of presenters were trying to encourage the Indian audience to take an active interest in Bitcoin mining as a means to profitability by introducing mining products and pitching the benefits of online exchanges where Bitcoins could be traded. The real question of how Bitcoin could benefit Indian systems was not dealt with and only briefly focussed on the concept of cashless payments as a whole.

The conference, as a first of its kind, joins Amsterdam and Singapore as a Global Bitcoin Conference, but wasn’t able to generate as much confidence in some attendees who were looking for a more India centric discussion. Bitcoin continues to deal with issues of domestic regulation and merchant support within India which is critical in making it a mainstream currency. The intense focus on trading reduces the potential of Bitcoin as currency and places it strictly in the world of a pseudo-currency, like shares that can be traded online for profit. The other focus is entirely based on inviting investment for mining activities without clearly explaining the true costs.
More conferences and meetups that deal with the real complexities of Bitcoin in India are needed and this conference was a basic start towards people networking and building trust.
A word of caution

It is important to point out that Bitcoins and the field of virtual currency in India holds a very alluring market for technologists, entrepreneurs and even fraudsters. The potential of cryptocurrencies presents many attractions but is still finding footing in India. The companies involved in the conference present a very optimistic view of the future and need to ignite interest from general users for any positive results - financial or otherwise.

Sponsors such as ButterflyLabs are deeply invested in selling high end technologies such as processor cards that are specifically made for Bitcoin mining. Others like BuySellBitco.in are major players in the online Bitcoin trading platforms that are business’ dependent on trading through their portal. The product offered by BTC Robot assures an unrealistic return on investment in exchange for a down payment for their software. The software does automated trading of Bitcoins online and is built to capitalise on speculative fluctuations of the currency. Interestingly BTC Robot - advocates a highly misinformed and extreme position on virtual currencies as a whole and considers Bitcoin a fertile market to make money rather than promote it as a viable currency.

One general reminder for all those who are interested in participating in the world of Bitcoin, whether for profit or as a believer in the new digital currency, is that the currency is in a very nascent stage of development in India. It is bound to attract all sorts of people who may or may not be genuine in their intentions. Even at conferences such as the one in Bangalore, most participants are interested in figuring out how best to leverage the interest in Bitcoin towards profitable means for themselves - whether it is by selling software, hardware or advice on how to use Bitcoins. There is nothing wrong with their commercial interests but users need to pay give special scrutiny to claims and make careful judgements about who they trust with their money.

Government Regulation

The Indian government has expressed great caution against the blind adoption of Bitcoin by Indians. As a result, it issued a circular that outlined its views on the phenomenon. Its important to note at this point that Bitcoin as a phenomenon is intended to thwart central control but this doesn’t ensure that governments can’t influence key aspects of its real world infrastructure such as taxation of earnings and regulation of exchanges.

In its circular, dated 24 December 2013, the RBI made a statement that it would not regulate any virtual currency which includes Bitcoin. The cir-
cular emphasised the risk taken by users, traders, and merchants in using the virtual currency. The RBI also clearly stated that it does not consider virtual currencies as valid mediums of payment due to its lack of regulation or central authority. They also pointed out its high potential as a medium of speculative trading due to its lack of intrinsic value in their judgement. The biggest concern on the part of the government in the RBI circular was two fold - the financial risk taken by users and the use of Bitcoins in illegal activities like money laundering.

The Income Tax department also took interest in the activities of Bitcoin exchange owner like BuySellBitco.in and RBITco and instigated raids on their organisations. The issue of how Bitcoin earnings can be or should be taxed is still under discussion with no clear guidelines being issued. As a result many business’ that work in online trading had to shutdown seeking clarification from regulators regarding the legality of their activities. So far no clear message has come forward from the government and a select few websites have begun operations again. Other websites like BuySellBitco.in are still shutdown waiting for the government.

The RBI and Income Tax departments investigations have placed many Bitcoin business’ on hold in India.

Until the government is able to come to a fixed position on how it will deal with Bitcoin and other virtual currencies, users who wish to liquidate their Bitcoins to other currencies will have a very hard time. As a result they might use the currency for online transactions, but due to lack of any online retailers in India who accept Bitcoins their options will remain limited. Indian users should stay watchful of government advisories, to protect themselves and their financial interests, as well as to make the most of Bitcoins while they can.
Chapter #08

The Bitcoin world is a dangerous place and many precautions are needed to make sure that your money is safe. In this chapter we give advice on how to manage your Bitcoins.

The practical world of Bitcoin is very much like the wild west. No rules, no laws, no protection from the law or support from the community. If you lose in the game, if you're cheated, if you make an error or have a technical glitch, you’re stuck with the consequences. Since Bitcoin is designed to work outside the legal system and be absolute in its activities Bitcoin users have to look out for their own interests. This process involves having to learn new ways of operating online.

Important Dos and Don’ts
and participating in the Bitcoin community. This chapter will point out some of the basics involved in self-protection for a regular user.

**Common Mistakes and Precautions**

**Wallet Management**

Bitcoins do not have a physical form and are stored virtually in wallets stored on your computer. These digital wallets serve the same purpose as a real one and just like real wallets they are vulnerable. There are a number of steps necessary to secure these digital wallets, most of which are common sense but are worth reminding.

As people shift further towards using Bitcoin’s its natural for the number of Bitcoins in a wallet to increase. It’s wise to ensure that not these Bitcoins are not stored in one wallet and instead divided amongst a number of wallets for protection. In case of theft or error, the likelihood of all wallets being lost becomes less and your investment is secured.

Particular care is necessary when dealing with multiple wallets and vast number of Bitcoins. The attitude should be similar to how cash is handled in the real world, with vigilance and care. In this way, it is also advisable that a share of your Bitcoin wallets be kept offline and all the wallets be regularly backed up. Just as you would set up restore points for your computer, it is necessary to make up to date backups of your wallets in case of loss.

![Wallet Management](image)

Wallets appear on devices as portal which can be used to send and receive Bitcoins. They are also available on certain mobile devices.
Encryption
In the digital world, encryption is the lock that protects your money. Wallets can also be encrypted so that even in case of theft or an online attack, they are not exploited and you can revert back to a backup. In order to ensure this various encryption measures can be taken, specially when sending copies of the wallet online, in backups and when using them on alien machines such as those at work. Not all systems are secure and the only thing protecting your money is the encryption on the wallets. For those specially paranoid, a encrypted wallets should be backed up in multiple locations so that complete and total loss is recoverable.

Without encryption for your wallets, your money is as easy to steal as smashing this piggy bank.

Password Protection
As citizens on the online community the importance of password protection has always been of concern. In case of Bitcoin management, this concern takes on a very tangible face - money. So it’s especially important that greater care be taken with wallet encryption password than with regular email or online websites.

The passwords used when encrypting wallets should be completely unique and not a recycled version of email or work passwords. In the case
of Bitcoin protection, complexity and difficulty are more crucial than ever. It's necessary to find a balance between complexity and recall - but if the password is easily remembered then there is a greater likelihood that it can be hacked. The need to be clever in password creation becomes very critical. It may even be necessary to have a copy of a complex password stored in hard-copy in the real world where more obvious protection can be given such as inside a locker etc.

**Machine Protection**

The machine used when operating online is similar to the safe that stores our valuables. If the safe gets stolen the money inside is lost to us as well. Similarly, the machine we use to access the internet and use our Bitcoins on need just as much security as the Bitcoins themselves. If our machines are compromised then it is more likely that our money is at risk.

For this reason all the advice that we usually can afford to ignore such as regular anti-virus update or the installing of questionable software needs to be given special attention. Its important to not use our Bitcoin wallet on any machine that we can't vouch for as being secure - this means machines at work, at a friends place, at cyber cafes etc. shouldn't be used to operate our wallets.

It is also important that we avoid illegal softwares, hacks, patches and other anonymous developer warez on the machines that we use for our Bitcoin wallets. These softwares are a vulnerability that can be exploited to attack our wallets for theft. In this regard, original operating systems should be used for Bitcoin wallets since they can be trusted more than pirated ones. These original systems can also be upgraded with security patches that ensure protection of the system and our money.

**Bitcoin Malware**

The most important threat to Bitcoin users, especially in India, is from malware that can infiltrate and steal from your wallet. India is amongst
the top six countries suffering from Bitcoin malware according to research by Trend Micro. Basic precautions become more urgent in this context and the use of unknown softwares becomes a greater threat. Even the use of unknown USBs, DVDs and other devices can pose a risk as they are vector points where malware can enter our system.

In the event of suspected attack its critical that a complete system wipe we done at the hard disk level and a clean operating system be installed. In addition to which it makes more sense to pay and use as good an antivirus and firewall program as possible but to not blindly give in to their assur-

![2013 Bitcoin Malware Trend](image)

The latest research shows the extreme rise in Bitcoin based malware resulting in millions of losses.

ances. Personal vigilance is the first step to system and Bitcoin security. In this case, programs that are no longer used should be uninstalled since malware can harm the system using vulnerabilities in those softwares. Even visiting questionable websites should be looked at and it is advisable that it should be done through virtual machines (VirtualBox).

**Bitcoin scam awareness**

Where there is money, there is crime and Bitcoin is no different. Given the key features of Bitcoin like anonymity, irreversible transactions and active currency exchanges, criminals are very keen on parting coins from their owners without fear of being caught. Various types of scams and tricks have been used in this venture. The biggest losses in the brief history of
this currency number in millions of dollars and demonstrate how fragile the new methods of this system require special care when being handled by newcomers.

The PayPal Buyer Exploit
An early scam in the Bitcoin evolution was the PayPal-Bitcoin scam where payments made over PayPal for purchasing Bitcoins were used to scam Bitcoin sellers. In India, it is possible a similar scam may arise so a brief review is necessary. A Bitcoin seller would be willing to accept payments in fiat currency online in exchange for a Bitcoin transfer using a service like PayPal. The deal would be made between buyer and seller with money escrowed in the PayPal account of the seller. The seller would then digitally send the Bitcoins to the buyers address. But after receiving it, the buyer would file a report with PayPal complaining that it had never received the Bitcoins. As per PayPal policy, since there is not traceable proof of transfer, the buyer will get the fiat currency back and the seller would have lost Bitcoins. Due to the infamy of this scam, the sale of Bitcoins using PayPal and similar services has seen a tremendous decline and virtually put an end to PayPal as a means of paying for Bitcoins.

Mining Hardware Scam
One of the key examples of Bitcoin scams comes from exploiting the desires of many people who want to become Bitcoin miners. Although a certain level of tech familiarity is necessary for anyone to venture into the world of Bitcoin mining, even the most careful people have been known to be scammed.

Although Bitcoin mining can be done even on a regular home computer it is not as profitable when compared to specialised mining rigs. These rigs are specifically designed to direct all processor computing power towards mining and employ high end processor chips and power supplies, which can cost tens of thousands of dollars. Given the promise of mining your own currency that is worth thousands per unit this seems like a viable deal for most miners but it is also the vulnerability exploited by scammers.
Many fraudulent websites offer hardware for Bitcoin mining claiming themselves to be the next generation of technology. In many cases this may be true but it is also one of the common ways of trying to defraud naive users. In many cases, these websites take advance payments for yet to be released rigs and then delay delivery or default completely without returning their customers money. It’s important to seek reviews of any website or equipment source before making any payments for future deliveries. Even long time active providers such as Butterfly Labs (that sponsored the Bitcoin Conference) have been accused by the Bitcoin community of irregular behaviour such as delayed delivery and product that’s not as claimed. Do your research.

Another risk to miners or even regular users is from malware and trojans that can slave your computer’s processor to work in the mining pool without any indication. Over 12,000 personal computers have already been infected by Bitcoin malware that makes them into virtual assets for criminals. Not only does this result in a severe slowdown of the infected system but also leaves the system vulnerable to other attacks.

Ponzi Scam
Bitcoin has itself been called a Ponzi scam since its inception but due to its decentralised nature it has proven to be nothing of the kind. However, the traditional Ponzi scam can still be used on the Bitcoin system without
many changes. The Ponzi scam is basically the offer by a third party to reward participants with high return on their investments. In the world of Bitcoin the scam works like so - an online business, an investment firm mostly, declares that if you store your Bitcoins with them they will give you an assured percentage of profit on a weekly or monthly basis. That means if you deposit 100 BTC with them, they will give you a return of 2-7 percent weekly. This is obviously a great deal but it is also a complete work of fiction.

But most users are not aware of how trading and Bitcoins work, and start off with a small investment. To their surprise they are rewarded as promised and decide to deposit even more with the service. But suddenly and unexpectedly the website or service stops returning any profit as well as responding to messages. It disappears with all deposits made and no trace of their existence. This is the basic model of the Ponzi scam and it defrauded countless people of over 26,000 BTC or roughly USD$ 26,000,000 dollars over 2011-12 in the form of the Bitcoin Savings and Trust scam.

**Physical Sale Scam**

A new scam, in areas where Bitcoin is still emerging, involves the sale of physical Bitcoins. Users are required to send their Bitcoins to the service providers address and in return they receive a freshly minted metal or gold coin that has the Bitcoin value stored on it in the form of an inscribed key number. However, most early users of Bitcoin are not clear on the nature of Bitcoin and fall prey to fake coins that can’t really be used in the real world. In certain cases, even the gold value equivalent coins are fake and the total funds deposited are stolen by the scam artists. Unfortunately, the irreversible nature of the Bitcoin system makes transactions with unknown persons and business’ a risky proposal. And even though an online directory of trusted vendors and merchants is available, countries that are not so well networked online, find themselves unrepresented leading to scams.

**Phishing Scam**

Phishing scams are a common plague in the virtual world - be it letters from your bank asking you for details or an African prince requiring bank details to transfer large sums of money. In the world of Bitcoin as well, this scam is used to interesting ends. Once people become active on the Bitcoin exchange using an email id and Bitcoin address, it isn’t too hard for criminals to figure out their targets. The Bitcoin version of this scam is based on
two methods - make users download malware or fool users into sending Bitcoins to incorrect address.

Criminals send out mass emails to thousands of email ids. Most emails seem innocuous and innocent, seemingly from people you may know. They usually have attachments or links to download files that seem relevant and important. But as is always the case, these files are trojan viruses or similar malware that can exploit and harm the user’s system and Bitcoin assets irreparably. As is always the case, its easy to avoid this scam by simply not opening attachments or clicking on links from unknown sources, irrespective of what the mail claims.

![Image of a fake website]

An example of old-school phishing scam – a fake website. Always make sure your URLs are secure and correct.

**Dangers for Bitcoin users**
The world of Bitcoin is just emerging and with no central regulatory authority it falls on the collective network of people to maintain order. Just as many of the Bitcoin protocols are based on community consensus, from the rules of the rewards to the use of Bitcoin clients, it is necessary for users to keep close ties to the community through forums for up to date information regarding risks and dangers.

But because of the very nature of the Bitcoin design, people who are use to the traditional way of dealing with money and online activities
need awareness of how Bitcoin needs a different approach. These changes can be dangerous if not understood well enough and cause serious loss of money to the users.

The number one thing to know about the dangers on Bitcoin is its easy allure to criminal activity. Not only in terms of scams and hacks but also how it is used by criminals to engage in trade that is difficult using normal currency. The recently shut down websites like Silk Road and the Sheep Marketplace were the most highly publicized examples of a digital black market. They attracted criminal activity such as the sale of drugs, weapons, assassinations and other illegal services by taking advantage of the untraceable nature of Bitcoin transactions.

Due to these activities most governments take a very cautious and highly scrutinised look at users of Bitcoin. In case of taxes and other legal money related requirements even the Indian government is investigating Bitcoin to discover how it can facilitate crime. It is very likely that innocent users may also be unwillingly caught up in this investigation and need to be prepared to explain themselves in case they are caught up in related issues.

Another key danger is the risk of losing your Bitcoin’s whether by accident or theft. Since there is no central authority and near anonymity in usage there is negligible chance of recovering lost Bitcoins. Unlike traditional banks, when you lose your credit or debit card, it is possible to block them and protect your account, but in case of Bitcoins once it is lost there is no recovery possible. Hundreds of people have lost thousands of Bitcoins, which is millions of dollars worth of losses simply due to accidents. And although insurance providers such as Lloyds of London have recently started providing protection for Bitcoin loss it is still an extra cost which bears down on users who are careless and not adequately prepared.

Many people would like to take advantage of the Bitcoin buzz and buy them as an investment. But as time has gone on since Bitcoin’s creation, it is no longer convenient for newcomers to buy Bitcoins as it was before. Even though there are valid Bitcoin exchanges active in India and abroad, they require credit cards or online bank transfers to be used. Although it is still possible to purchase Bitcoins from individuals, India currently is in a freeze where the only way to purchase Bitcoins is directly through a trusted first hand source. Once the Indian online exchanges are active people with online banking with select banks will be able to buy Bitcoins again if the government allows.
Another danger of Bitcoin users in India is its acceptability and therefore risk to fraud. There are no known businesses operating in India which accept Bitcoin as payment. Only the trading exchanges accept Bitcoin as a transaction fee. So most Indians would be considering Bitcoin as a speculative trading security which in itself poses many risks. In addition to which, the newness of the currency makes it possible for many flaws to emerge that can be its undoing, specially the risk of an ownership majority, which would allow a small group of people undue advantage of manufacturing and trading Bitcoins at high sales prices. This has almost happened with Bitcoin once before.

**Speculation Knowledge**

One of the features that makes people interested in Bitcoin is how it can increased in value tremendously over the past year. This radical increase in value makes it seem like a worthwhile investment which can yield significant financial results. This is true. But it is also a great risk.

Speculation trading has a long history in other analog markets such as gold, shares, bonds, derivatives and commodities. The behaviours witnessed in all these markets over decades of activity point towards certain trends that need to be considered. First and foremost of this is - speculation is identical to gambling in most respects. Although a specialised group of people such as stock traders and market analysts are able to bring an element of rationality to this gambling through research and investigation, the rules don’t apply to Bitcoin. There is no such thing as a trend, primarily due to two factors - the brief existence of Bitcoin and its absolute reliance on supply and demand.

The idea behind speculation trading is simple - to buy at a low price and sell at a higher one. However, there is no guarantee of knowledge regarding when a higher price is going to come or if the value will drop instead of
rising. To resolve this there may be offers from specialist business' that claim to be able to perform this service for users - which is in itself a risk as we have discussed before, trusting others with your Bitcoins is a major danger.

And since Bitcoin isn't like company shares or commodities there are no market indicators that can be used to rationally decide what is the best time to buy or sell Bitcoins for investments. The only indicator that has seen definite results in altering the market is user trust. Whenever users have felt insecure about the validity of Bitcoin, the prices have radically dropped. This was the case when the government of China and India issued warnings against Bitcoin usage, the result was a shocking 30-50 percent drop in value with a very slow and gradual recovery. If any government was to specially endorse Bitcoins, the results are expected to be opposite but there is no legal way to plan for that outcome.

Other influence that can suddenly alter the value of the Bitcoin is its supply. If suddenly a large number of miners or a single large miner devotes great processing power towards Bitcoin and the rate of Bitcoin generation is boosted, the effects can prove volatile for the value. The system is designed for slower mining as time moves forward, but if technological advancements undo this parameter then the fluctuations in value are assured.

The most important thing to realise about Bitcoin and speculation is that unless there is an assured knowledge of what will influence Bitcoin, all trading activities are simply gambling. It is better instead to think of Bitcoin as what it was designed to be - a currency. If someone is not a professional trader in Indian rupees, US dollars, Japanese Yen and other currencies, then it’s unlikely they will have the ability or the skill to profit when speculating Bitcoins. It is better to adopt it as an efficient means to conduct online payments and save money on transaction costs. 

Is Bitcoin the end of the line for virtual currencies or just the beginning? We play soothsayer in this final chapter and try to predict the future.

It is very easy for most people to dismiss Bitcoin as something that is nothing more than a fad. This is not an invalid argument, since history has shown that people can be obsessed with items that promise profit and change but for short periods of time. Be it something as simple as Pokemon trading cards (worth thousands of dollars) or digital gold. But
the future of virtual currency has something that no other item in the past has been able to demonstrate - community trust.

Bitcoin is built on the pooled trust of its users - from miners who dedicate processing power in exchange for the mined coins and transaction fees, to the everyday user who wishes to make payments hassle free without going through online payment fees. The future of Bitcoin is therefore built on how the trust of the members is rewarded by the collective behaviour of the community - from speculative traders effecting the price to criminals who abuse the system. Above all else, this is the key factor that will determine the future of Bitcoin.

Factors effecting digital currency adoption
Digital currencies can only function adequately in predominantly digital nations. Nations such as those in the Americas, Europe and other advanced nations, are primed to actually shift to a partially virtual currency model. But as long as the internet inclusivity of developing nations remains low, the likelihood that they will adopt Bitcoins in any meaningful way remains limited. This is not to say that a small, core group of users can't participate in the Bitcoin economy via the internet but it does mean that unlike cafe’s in Canada, there will be no paying for coffee with Bitcoins.

Internet adoption although on the rise in India is still closer to 10% of population, lagging behind many other countries in Asia.
Another key factor of Bitcoin adoption in the long run is the presumed eventual stabilization of its value. As long as most Bitcoin users retain the speculative trading aspect of the currency, Bitcoin will not be able to find any meaningful usage in the broader economy. The constant fluctuation in prices will distance it from business users who rely on a stable currency in order to conduct their operations since it’s not reasonable for a business to constantly change the price of its goods and services based on the moment to moment exchange rate of Bitcoin to fiat currency.

The possible solution to this dilemma is if many participants in a business set up - from employees to customers, vendors to utility companies, begin accepting Bitcoin as payment. In such a scenario the normalised usage and flow of the currency in the economy would automatically stabilize the value of the Bitcoin. Instead of a constantly fluctuating price tag on good online, we would find that Bitcoin has become the standard currency that doesn’t change based on its exchange rate. This is a feasible reality in select first world countries whose financial systems aren’t as strictly regulated but for the majority of the world this outcome doesn’t seem likely.

In countries such as India, the adoption of Bitcoins may prove to be highly focused in urban, educated and computer literate areas. Since the use of digital wallets, mobile money and password encryption has barely become mainstream in this part of the world Bitcoin could find adoption in a purely online scale where it becomes a relative substitute to PayPal or credit card payments.

However this shift can only occur if the trust index on online identities is maintained as it is on e-commerce websites like eBay, where even anonymous looking members have a public track record of their activities. A similar trust indicator would ensure that when a buyer makes online payment using Bitcoin in advance of receiving a product, they do so to a trustworthy seller who will not default on the deal. This trust index would be a critical aspect of the modern virtual currency, since payments that can not be reversed will not be risked to first timers and only to reputed merchants.

**International financial regulation**

Bitcoin can be halted in its tracks in most parts of the world where regulation requirements are high. Major countries that participate today such as China, Japan and Europe are very careful of their internal economies and exert strict control over their internet infrastructure as well as traditional financial institutions. If they decide that Bitcoin is detrimental to
their nations then they can easily have them blocked by not allowing currency conversion between Bitcoins and local currency.

This can have two possible outcomes - firstly, people who use Bitcoins partially would be forced to limit their Bitcoin transactions to only the online world due to its lack of usability in their real life, and secondly, it may force people to shift to a predominantly Bitcoin oriented lifestyle. This second possibility can only exist if there are enough merchants and service providers who are willing to accept Bitcoins for services. But given the abrupt nature of the currency so far and its conflict with governments in general, it is unlikely that Bitcoin would find mainstream existence if a government decides to kill it.

Financial regulations are intended to retain control over a nation's wealth and that includes the wealth of its citizens. From taxes on all sorts of money, such as income, sales, duties etc. Bitcoin is a way for people to cut out the government from its finances. In India, this isn't that significant of an issue due to the extreme minority of people who access the internet and therefore can use Bitcoin.

However if a large number of taxpayers in the top bracket, who are technologically friendly, start using Bitcoin and other alternative currencies to dodge their dues to the tax department, then it isn't hard for the government to shut down access to Bitcoin. Since the Bitcoin community is so small it wouldn't be difficult for governments to ignore it on the grounds of protecting the nation's interest.

Abroad however the issues may be far more complex since access to the internet and online censorship is highly criticized by the citizens of those nations.

**Risks and benefits**

Bitcoin is at a very critical stage of its evolution. It has already shown that for some it can yield tremendous profit ever since its price rapidly went up in a short period of time, and in other cases it has shown how easily such fortunes are lost. The risks are inherent but in the long run there are only
Future of Bitcoins and Alternative Currencies

A handful of risks that can affect users of all types - lack of community trust in the currency and the unknown reactions from governments.

Even though the community is highly active online and maintains a check on fraudulent activities by reporting them in forums, there is still no authority that can be relied on for the security of any investment made on using Bitcoins. This gap in the system invites trouble and even though it’s a fraction of the whole, it is still enough to alienate a lot of potential users who still don’t understand the currency clearly.

As time goes on various possible outcomes or a variation of them may occur. They can be generalised in the following -

1. People only use Bitcoins in select circumstances
2. People use Bitcoins insurance to offset risks
3. A new range of Bitcoin services pop up that help offset fluctuating prices through financial instruments like futures and put options
4. Bitcoin escrow services attempt to secure trades so that users aren’t defrauded
5. Government disincentives businesses from using Bitcoin
6. It becomes expensive for Bitcoin service providers such as exchanges to continue operations
7. Bitcoin becomes a purely underground currency with little mainstream acceptance
8. The government completely bans Bitcoin and other unregulated virtual currencies

It’s important to note that any positive measures that help users, such as the first four mentioned above would mean an increased cost of transaction,
due to the payment of insurance premiums and other costs for security. These add on payments would make Bitcoin at par with using credit cards in terms so transaction fees and make the whole point of the currency moot.

In the case of the latter four cases Bitcoin users could find their options reducing and since a currency is only as dependent as its acceptance, we would observe a massive crash in the price of the currency. Hundreds, if not thousands, of people would find themselves holding worthless alphanumeric numbers that aren’t worth anything in trade. Online merchants would be the first indicator of this shift as they are the most highly dependent on real world currencies. If governments actively oppose virtual currencies instead of remaining neutral or supportive then its even more likely Bitcoin will not even have value on the blackmarket.

**A look into the financial crystal ball**

The stark reality is this - Bitcoin is a revolutionary innovation that has befuddled regulators and given a new sense of freedom to its users. But all these changes have come at a significant loss of trust by the non-technological community as well as a very anti-regulatory attitude that is built into the currency. These opposing factors ensure that even at the worst of times there will always be Bitcoin users in the world even if they may not be in such large quantities.

Just as even today there are users on the darknet who live completely innocent lives online and do so just to have the freedom of anonymity. The question is of trust and culture. In Eastern nations, there is great mistrust of people who only look out for themselves and don’t depend on communities. Just as in Western nations, collective groups are not trusted specially in finance and business, and being mistrustful is considered a virtue since the individual is king. These conflicts of local culture make it unlikely that the features of Bitcoin and similar currencies will make it acceptable to a global user base.

This doesn’t mean that Bitcoin is sure to fail - in fact it may discover yet unrealised features such as becoming component of vast business’ such as the Steam online infrastructure that already witness’

Many claim to know the future; we discuss the many possible variations.
currency like exchanges and online payments for games. If an online gaming portal could find a way of integrating Bitcoin protocol payment systems, Bitcoin could find a dedicated community of users who understand its technological aspects and know how to use it effectively.

The very likely outcome we are sure to see in the future is financial companies, banks and governments to study and adopt the Bitcoin protocol for its socially beneficial features. Credit card companies could easily establish a version of the Bitcoin protocol where users of all banks and holders of any credit cards could instantly and immediately make payments to each other without incurring transaction costs.

Credit cards and banks could also adopt the Bitcoin protocol internally and provide the hybrid advantages of fast, efficient and free transactions with the security of knowing that your money is safe from sudden loss. This adaptive attitude by financial companies could thereby usurp the current popularity of the Bitcoin system. It is obvious that Bitcoin isn’t made for all types of economies, specially developing economies like India where an internet connection is a rarity and trust of technology is predominantly low. In such places the positive adaptation of the Bitcoin protocol could prove revolutionary specially if its mobile applications are verified. The socially positive possibilities are endless if innovated responsibly.

**Bitcoin is just the beginning**

The history of the internet and money was not planned or well executed, with too many private players taking advantage of the new medium to
overcharge customers for services that are essentially free. We see a similar example of this in how people pay for SMSes when in fact they do not cost telecom companies anything to provide them to subscribers. They are in reality the cream on the cake for telecom companies but people continued to use and pay for them until mobile internet became an option. This shift in technology allowed users to choose Whatsapp and other net based messaging services at negligible costs. In order to adapt to this shift, telecom companies are now offering Whatsapp exclusive mobile net options hoping to continue to make profit in this new system.

The absence of knowledge regarding technology and innovations is often used by private players to take advantage of their naivety. This institutional behaviour and its subsequent effects, in the form of financial meltdowns in first world nations, led to the inspiration behind Bitcoin. A currency that couldn’t fall prey to the deceptive nature of people, who would otherwise artificially inflate currency value or engage in practices that left money worthless in the hands of their citizens. This mistrust led to the acceptance of Bitcoin, since it suddenly became easier to trust in computer code and math, than in another human being.

As time has gone on people have come to expect less and less from each other. This lack of trust has manifested itself into Bitcoin and the general rise of virtual currencies. However, by placing the responsibility of one’s own money in no-one’s hands but our own and our technology, we demonstrate a very fearful attitude towards the community we live in as a whole. There are numerous situations where we are forced to trust somebody with our welfare which means allowing them access to our assets. Luckily we have also found means of misuse and the law exists to correct any wrong
doings. In the world of Bitcoin this would be impossible. You won’t be able to trust anyone when it comes to money.

The current version of the Bitcoin protocol doesn’t account for the positive side of trust when it comes to people and only uses trust in machines and mathematics to present its cause. This is a very powerful advantage for Bitcoin but also its greatest weakness. But that isn’t the end. Bitcoin is created to be organic and adaptive as long as the majority of people accept those changes. It is not wrong to be hopeful that yet to launch currencies like Buttercoin and Laxmicoin will be built keeping in mind the Asian sensibility - one that places the ideal of individual freedom and community faith side by side. How these two balance out in the future, only time will tell, but it is hard to imagine virtual currency replacing paper money anytime soon - how can it when even digital books have barely even begun to replace paper ones?
NEWS AND REVIEWS
Comprehensive news, unbiased reviews and ratings to help you make the right purchase

DOWNLOADS
Check out the latest software downloads, games for your Windows, Linux, Mac and PDA/mobiles

All this and more in the world of Technology

VISIT NOW www.thinkdigit.com
Join 140K+ members of the digit community

facebook

digit

Your favourite magazine on your social network. Interact with thousands of fellow Digit readers.

facebook

1 Think Gadgets

An active community for those of you who love mobiles, laptops, cameras and other gadgets. Learn and share more on technology.

facebook

Glad to be a Programmer

If you enjoy writing code, this community is for you. Be a part and find your way through development.

devworx

devworx, a niche community for software developers in India, is supported by 9.9 Media, publishers of Digit