

MAY 2018 • Vol. 4 • Issue 2

MONTHLY • Pages 64

₹ 200

RNI No.: DELENG/2015/67140; Published on: Every month; Posted at Lodi Road HPO, New Delhi on 9-10th of every month

THE AWARE CONSUMER

(SUBSCRIBER COPY NOT FOR RESALE)

www.consumerconexion.org

Report

Cryptocurrencies:
Dawn Of A
New Economy

Out Of The Box

How Cryptocurrencies
Emerged As A Side
Product Of Digital Cash

The Last Mile

Is Bitcoin
A Waste Of Electricity,
Or Something Worse ?



Changing The World ...

CRYPTOCURRENCY

For The Better Or Worse ?!

PLUS

ROUND UP • HORIZONS • IN FOCUS



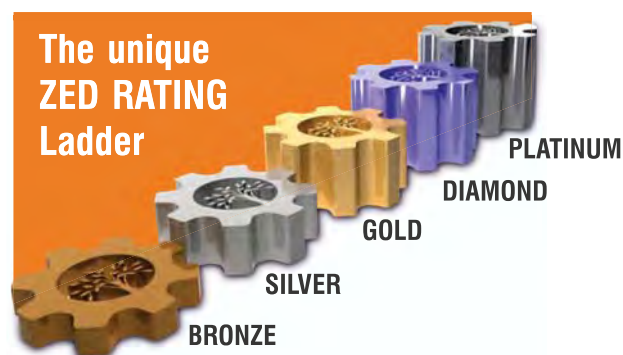
“Let’s think about making our product which has ‘Zero Defect’; so that it does not come back (get rejected) from the world market and ‘Zero Effect’ so that the manufacturing does not have an adverse effect on our environment”

SHRI NARENDRA MODI
Hon’ble Prime Minister



Certification Scheme

A roadmap to
World-class manufacturing



HIGHLIGHTS

- ⚙️ A scheme by Ministry of MSME, Govt. of India
- ⚙️ Certification on the systems and processes of MSMEs
- ⚙️ Handholding MSMEs towards world class manufacturing
- ⚙️ Special emphasis on MSMEs supplying to Defence Sector
- ⚙️ Direct subsidy to participating MSMEs
- ⚙️ Creating a credible database of MSMEs for OEMS/CPSUs/Foreign Investors under “Make in India initiative”
- ⚙️ Quality Council of India (QCI) to function as the NMIU (National Monitoring and Implementing Unit) of the scheme

Free Registration at
www.zed.org.in

VIEWPOINT

BEJON KUMAR MISRA | bejonmisra@consumerconexion.org

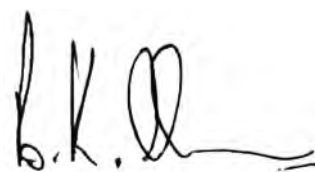
A Greater Fool's Gold

FEW MONTHS BACK a plague of kittens brought down one of the most fashionable cryptocurrencies on the internet. This might not have been news, except that the cryptocurrency, Ethereum, bills itself as “the world computer” – a distributed program that can replace large parts of both the legitimate banking system and the legal system itself, since contracts can be written into computer code. Unless, that is, Ethereum becomes the plaything of an imaginary kitten. Like all other cryptocurrencies that have appeared in the wake of bitcoin, and like bitcoin itself, Ethereum is useless as a medium of exchange because the price fluctuates violently and unpredictably. But it turns out to be an excellent medium for the propagation of imaginary kittens and when a small Canadian company introduced a game that let players buy and breed cartoon cats, the resulting popularity brought the whole network briefly to its knees. Had Ethereum been a real currency, this would have been as if the Beanie Baby craze of the last century had crashed the world's credit card system. But of course Ethereum is not a real currency, and neither is bitcoin; nor are Ripple, Monero, Litecoin, Dogecoin, or any of the other thousands of cryptocurrencies that are the focus of intense speculation today.

They are the latest manifestation of the eternal dream that we could, by magic, become really rich really quickly. Why, if only you had bought bitcoin a year ago, they would now be worth 16 or 17 times as much, or, last week, only 13 times as much. What could possibly go wrong? Nonetheless the bubble must one day pop and the fool's gold vanish, leaving only fools.

The central paradox of all these currencies is that we're told they have eliminated the need for trust between humans and replaced it by mathematical guarantees; but all their tradeable value depends on blind faith and ignorance of computer code. Only sometime back a Google researcher discovered a hole in some software widely used to store bitcoins which would leak all their contents to any suitably malicious webpage that the owner visited. This had in fact been pointed out to the developers months ago, but they had not bothered to fix it. Flaws in the code of Ethereum led to the theft of \$30m in the summer of 2016 and the disappearance of \$170m last autumn, though all these sums are entirely notional. Even software built by gigantic, legitimate companies can turn out to have catastrophic bugs in it, as we learned from the publication of the Meltdown and Spectre flaws, which between them affect almost all modern computer chips.

There is even less reason to trust software developed by small teams of programmers who hope both to become insanely rich and to circumvent all efforts by governments to control them – and that is how all cryptocurrencies have been built. But there is not much use in sober realism here. So long as ordinary people can expect to make their fortunes overnight, they will step up to the gaming table and play – at least while the cryptokittens are away.



Flaws in the code of Ethereum led to the theft of \$30m in the summer of 2016 and the disappearance of \$170m last autumn, though all these sums are entirely notional.



Message from the Editor-in-Chief

POOJA KHAITAN

pooja@jagorahakjago.com

Is It Driven By Greed?

THERE WAS A time when “a penny saved is a penny earned” was all anyone needed to know about money. That is so 20th century.

Money, as we've known it (and yearned for it), relies on centralization for its print, its banks and for its insurance. But toward the end of the last century some began to see the centralization of money as monetary “monopoly,” and that unease begat cryptocurrency, the go-to coin for those seeking an alternative to money tied to government controls. Cryptocurrencies live on a cloud, waiting to be summoned to Earth.

Cryptocurrencies such as Bitcoin and, more recently, Ripple, were eagerly embraced. Millennials, perhaps the segment of society most susceptible to the siren call of money shielded from prying authority, were lured in great numbers to the novelty of cryptocurrencies, freedom and perceived easy path to wealth.

Now, more than ever before is a time to be thinking about cryptocurrencies. Over the past few years, cryptocurrency has grown exponentially

because of its attractiveness to people looking to use this alternative money. Bitcoin, the best known of the new cryptocurrencies, is one of those words surrounded by automatic buzz, in part because everyone's so excited about its potential.

And it's no surprise that cryptocurrencies are exciting, overall. Because they're decentralized (no banks!), anonymous and electric, they've got the potential to change the world as we know it. The apparently endless rise in the prices of cryptocurrencies is a monument to greed and gullibility.

Yes, it's driven by greed — but the mania for cryptocurrency could wind up building something much more important than wealth.

INSIDE

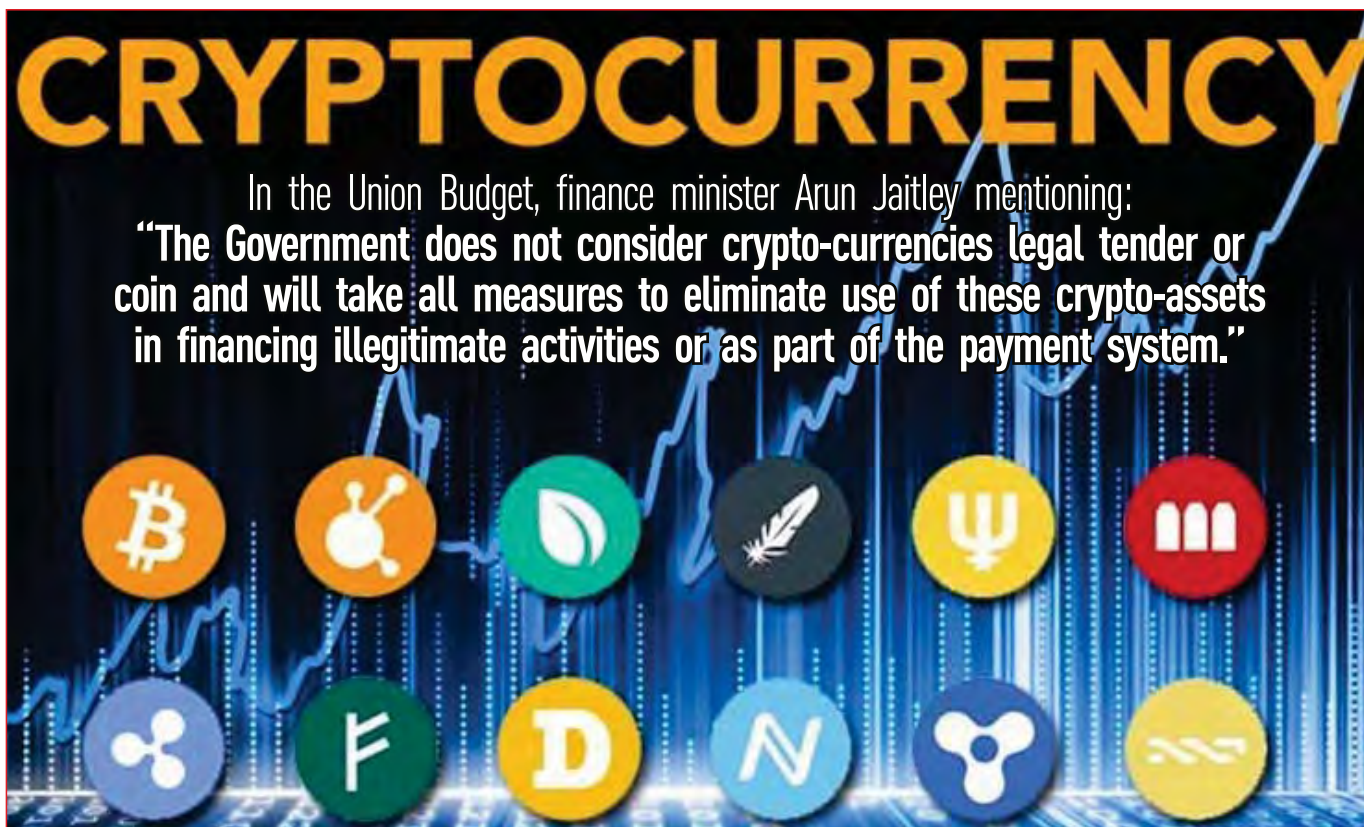
REGULARS

03 | VIEWPOINT

07 | ROUNDUP

41 | AFTERWORD

THE AWARE CONSUMER | MAY 2018



RESEARCH FEATURE

17 | All About Cryptocurrency



A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets.

HORIZON

33 | CRYPTOCURRENCIES AS A DISRUPTIVE INNOVATION



There have been numerous instances where disruptive technologies have displaced well-established competitors, WhatsApp displacing Short Messaging Service (SMS) being one such example.

GOVERNMENT PERSPECTIVE



37 | END OF THE ROAD FOR CRYPTOCURRENCIES IN INDIA?

While some welcomed the RBI's move, others stressed on the need for more regulation rather than a ban.

OUT OF THE BOX

44 | HOW CRYPTOCURRENCIES EMERGED AS A SIDE PRODUCT OF DIGITAL CASH



Few people know, but cryptocurrencies emerged as a side product of another invention. Satoshi Nakamoto, the unknown inventor of Bitcoin, the first and still most important cryptocurrency, never intended to invent a currency.

MY MARKET

48 | WHAT THE CENTRAL BANKS ARE SAYING ABOUT CRYPTOCURRENCIES



Eight years since the birth of bitcoin, central banks around the world are increasingly recognizing the potential upsides and downsides of digital currencies.

OPINION

53 | BLOCKCHAIN IN INDIA: MOVING BEYOND THE RHETORIC



India is keen to work on innovative solutions to promote inclusion, to empower masses and to do so at a faster pace.

THE LAST MILE

56 | IS BITCOIN A WASTE OF ELECTRICITY, OR SOMETHING WORSE?



"It appears that much of our evolving digital infrastructure is devoted to activities, like the proliferation of cybercoins, that are worse than frivolous," said James McAndrews, the former head of research at the Federal Reserve Bank of New York.

IN FOCUS

59 | 10 INCREDIBLE USES FOR CRYPTOCURRENCY AND BLOCKCHAIN YOU PROBABLY HAVEN'T THOUGHT OF



Cryptocurrency to battle election fraud? De-corrupt charities? Make the world greener? Who knew? Now, more than ever before is a time to be thinking about cryptocurrencies.

THE AWARE CONSUMER

UNLOCKING CONSUMER POTENTIAL
www.consumerconexion.org

MAY 2018 • Vol. 4 • Issue 2

Bejon Kumar Misra
PUBLISHER

Address: F - 9, Second Floor, Kailash Colony,
New Delhi - 110048
E-mail: bejonmisra@consumerconexion.org

EDITOR-IN-CHIEF
Pooja Khaitan

EDITORIAL CONSULTANTS
Suman Misra
Akanksha
Maanav Khaitan
Debaratti Dey
Pyush Misra

DESIGNER: Galaxy
DESIGN CONSULTANT: Maanav Khaitan

WEB DESIGNER:
Manish Mohan
Ebrahim Bhanpurawala

The AWARE CONSUMER
is printed and published by
Bejon Kumar Misra
at F - 9, Second Floor, Kailash Colony,
New Delhi - 110048 and printed at
M/s. Spectrum Printing Press (P) Ltd.,
Shed No. 23, Computer Complex,
DSIDC Scheme I, Okhla Phase II,
New Delhi - 110020

Place of Publication: E - 45, Ground Floor,
Greater Kailash Enclave - I, New Delhi-110048

For any queries, please contact us at
pooja@jaggrahakjago.com
Phone: 011-26271421/22/23

Total number of pages - 64, Including Covers

Material in this publication may not be
reproduced in any form without the written
permission of the Editor & Publisher.

DISCLAIMER: The views expressed in this
magazine are solely those of the author in his/her
private capacity and do not in any way represent
the views of the Editor & Publisher.



Please Recycle
This Magazine
And Remove
Inserts Before
Recycling

MR. GEORGE SOROS

HON FBA, HUNGARIAN-AMERICAN INVESTOR, BUSINESS MAGNATE, PHILANTHROPIST, POLITICAL ACTIVIST & AUTHOR

According to Bloomberg, a member of his family office received internal approval to trade cryptocurrencies, an asset that most traditional money managers have avoided due to the sector's limited track record, lack of regulation, and volatility.



ROUNDUP

BITCOIN is the first decentralized digital currency, as the system works without a central bank or single administrator



UNDERSTANDING THE IMPACT OF CRYPTOCURRENCY AND BITCOIN

HISTORY

In 1983 the American cryptographer David Chaum conceived an anonymous cryptographic electronic money called ecash. Later, in 1995, he implemented it through Digicash, an early form of cryptographic electronic payments which required user software in order to withdraw notes from a bank and designate specific encrypted keys before it can be sent to a recipient. This allowed the digital currency to be untraceable by the issuing bank, the government, or a third party.



DATA BRIEFING

A 2016 joint report from Coinbase and ARK Invest estimates that **54%** of Coinbase users use bitcoin strictly as an investment.

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

In 1998, Wei Dai published a description of "b-money", an anonymous, distributed electronic cash system. Shortly thereafter, Nick Szabo created "bit gold". Like bitcoin and other cryptocurrencies that would follow it, bit gold (not to be confused with the later gold-based exchange, BitGold) was an electronic currency system which required users to complete a proof of work function with solutions being

cryptographically put together and published. A currency system based on a reusable proof of work was later created by Hal Finney who followed the work of Dai and Szabo.

The first decentralized cryptocurrency, bitcoin, was created in 2009 by pseudonymous developer Satoshi Nakamoto. It used SHA-256, a cryptographic hash function, as its proof-of-work scheme. In April 2011, Namecoin was created as an attempt at forming a decentralized DNS, which would make internet censorship very difficult. Soon after, in October 2011, Litecoin was released. It was the first successful cryptocurrency to use scrypt as its hash function instead of SHA-256.



BITCOIN

LAUNCHED: 2009

Bitcoin is the first ever cryptocurrency that followed blockchain and cryptography technique. Bitcoin is an experimental, decentralized digital currency. Now it has become more worthy than an ounce of gold.



RIPPLE

LAUNCHED: 2011

Ripple is a fundamental infrastructure that improves the payment process. It is a neutral Internet-based protocol for communicating banks and payment systems. Banks can use it as a general ledger to clear and settle transactions.



NXT TECH

LAUNCHED: 2013

NXT is a radically enhanced cryptocurrency built from scratch, to deliver an exclusive and decentralized financial platform. It revealed new ways to use digital cash as well as share transfers. Nxt enables alias system, voting system as well as monetary system.



ETHEREUM

LAUNCHED: 2014

Ethereum is an open source platform for smart contracts built on top of block chain technology. It enables blockchain-based "decentralized autonomous organizations" (DAOs). The mining process of Ethereum completely depends up on Geth.

BITCOIN ATMs

Gareth Murphy, a senior central banking officer has stated "widespread use [of cryptocurrency] would also make it more difficult for statistical agencies to gather data on economic activity, which are used by governments to steer the economy". He cautioned that virtual currencies pose a new challenge to central banks' control over the important functions of monetary and exchange rate policy.

Jordan Kelley, founder of Robocoin, launched the first bitcoin ATM in the United States on February 20, 2014. The kiosk installed in Austin, Texas is similar to bank ATMs but has scanners to read government-issued identification such as a driver's license or a passport to confirm users' identities. By September 2017 1574 bitcoin ATMs were installed around the world with an average fee of 9.05%. An average of 3 bitcoin ATMs were being installed per day in September 2017. ▶



Bitcoin slumps to month's low after Google's decision to ban cryptocurrency ads from June

THE BAN WILL come into effect as Google revises its financial services policy to restrict the advertisement of Contracts for Difference, rolling spot forex, and financial spread betting.

On the Ides of March, Bitcoin, world's largest cryptocurrency, dropped to month's low after Google announced that it will ban the cryptocurrency related advertisements from June 2018. At the time of reporting, the currency was trading at USD 8,250, recovering slightly from the low of USD 7,783. The ban will come into effect as Google revises its financial services policy to restrict the advertisement of Contracts for Difference, rolling spot forex, and financial spread betting.

The company said that ads for binary options and synonymous products, cryptocurrencies and related content, including but not limited to initial coin offerings, cryptocurrency exchanges, cryptocurrency wallets, and cryptocurrency trading advice will no longer be allowed to serve.

"Advertisers offering Contracts for Difference,



rolling spot forex, and financial spread betting will be required to be certified by Google before they can advertise through AdWords. Certification is only available in certain countries," Google said.

In January, Google's primary rival in the advertisement industry, Facebook had banned cryptocurrency ads saying, misleading or deceptive ads have no place on Facebook.

"We want people to continue to discover and learn about new products and services through Facebook ads without fear of scams or deception. That said, there are many companies who are advertising binary options, ICOs and cryptocurrencies that are not currently operating in good faith," Rob Leathern, Product Management Director had said then.

As per a report, these two companies share more than half of online advertising space, revenue-wise. The addition of cryptocurrencies to the banned list of these two giants could be a setback for entities dealing in them. ▶

IMPACT OF CRYPTOCURRENCY & BITCOIN



Bitcoin still remains the most popular form of digital currency, since its reach is widespread and is accepted by many businesses and retailers alike.

OVER THE LAST few years, the term cryptocurrency has rapidly gained visibility in the public eye. In today's day and age, cryptocurrency is fast becoming essential to people who value privacy, and for whom the idea of using cryptography to control the creation and distribution of money does not sound too far-fetched.

Today, cryptocurrency, led by Bitcoin, Litcoin, Ether, etc. are taking the financial world by storm as more people invest and buy these currencies. At the same time, there is still widespread confusion and bias which retracts for the overall effectiveness of Cryptocurrency. Educating users about such alternative forms of currency is extremely important given its volatile nature. In this article, we will try to provide a holistic outlook towards Cryptocurrency and how it's affecting the world we know today.

Why Use Cryptocurrency?

Bitcoin is the most popular cryptocurrency which has seen a massive success. There are other cryptocurrencies such as Ripple, Litecoin, Peercoin, etc. for people to transact in. But for every successful cryptocurrency, there are others which have died a slow death because no one bothered to use them, and a cryptocurrency is only as strong as its users. Some of the salient features of Cryptocurrency include -

- Cryptocurrency can be converted into other forms of currency and deposited into user's accounts at a lightning speed
- Most Cryptocurrency can be transacted anonymously, and can be used as discreet online cash anywhere in the world. Users therefore do not have to pay for any currency conversion fees
- While not 100% immune from theft, Cryptocurrency is generally safe to use and difficult for malicious hackers to break
- Bitcoin and other Cryptocurrency can be saved offline either in a "paper" wallet or on a removable storage hard drive which can be disconnected from the internet when not in use

Bitcoin - A Glimpse into the Future

2016 was the year of Bitcoin, and saw this digital currency grow almost 79% as compared to Russia's Ruble and Brazil's Real, the world's foremost hard currencies. As a result, it emerged as a better bet for investors while beating foreign exchange trade, stock exchange trade, and commodity contracts. There are many reasons why the impact of Bitcoin is exceptionally relevant today, and why the Cryptocurrency of 2018 is now here to stay. These include -

1 Reduced Remittance

Many governments around the world are implementing isolationist policies which restrict remittances made from other countries or vice versa either by making the charges too high or by writing new regulations. This fear of not being able to send money to family members and others is driving more people towards digital Cryptocurrency, chief amongst them being Bitcoin.

2 Control Over Capital

Many sovereign currencies and their usage outside of their home country are being regulated and restricted to an extent, thereby driving the demand for Bitcoin. For example, the Chinese government recently made it tougher for people as well as businesses to spend the nation's currency overseas, thereby trapping liquidity. As a result, options such as Bitcoin have gained immense popularity in China.

3 Better Acceptance

Today, more consumers are using Bitcoins than ever before, and that is because more legitimate businesses and companies have started accepting them as a form of payment. Today, online shoppers and investors are using bitcoins regularly, and 2016 saw 1.1 million bitcoin wallets being added and used.

4 Corruption Crackdown

Although unfortunate, digital Cryptocurrency such as Bitcoin are now also seeing more usage because of the crackdown on corruption in many countries. Both India and Venezuela banned their highest denomination and still-circulating bank notes in order to make it tougher to pay bribes and make accumulated black money useless. But that also boosted the demand for Bitcoins in such countries, enabling them to send and receive cash without having to answer to the authorities.

The Real-world Impact of Virtual Money

While Cryptocurrency and its usage is at an all-time high, so are the misconceptions about it. Most people still seem to ask - Why use Bitcoin? Since such currencies use different algorithms and are traded in unconventional ways, it is important to lookout for some important characteristics before investing in Bitcoin or others of its ilk. This includes-

- **Daily Trading Volume and Overall Market Capitalization**

Market capitalization of a cryptocurrency is the total worth of all its forms which are currently in circulation. New forms of Cryptocurrency might not be widely available, and therefore might not have high market capitalization. Similar to this is the daily trading volume, and a cryptocurrency which has higher trading volume than the others is considered more successful.

- **Verification Channels**

Each cryptocurrency has its own verification method. One of the most common methods for verification is called "Proof of Work". Herein, to verify a transaction, a computer has to spend time and computing power to solve difficult

mathematical problems. On the other hand, "Proof of Stake" method allows users with the largest share of the cryptocurrency to verify the transactions, which requires far less computing power.

- **Acceptance of Cryptocurrency**

Unless a cryptocurrency is not accepted by major retailers or other businesses that you deal with, it doesn't stand much use. That is why Bitcoin still remains the most popular form of digital currency, since its reach is widespread and is accepted by many businesses and retailers alike.

Toning Down the Frenzy - Challenges Ahead for Bitcoin

While Bitcoin's astronomical growth cannot be understated, Cryptocurrency in general have several challenges to meet before finding universal acceptance. These challenges include -

- **Safety and Reliability**

Purely based on its digital form, Bitcoin and other types of Cryptocurrencies are nowadays the favorite mode of payment for both hackers and criminals because of the air of anonymity it lends. This instantly makes the general populace weary of using it. In 2014, Mt. Gox, the largest Bitcoin exchange was hacked and robbed of almost \$69 million, thereby bankrupting the whole exchange. While the people who lost money have now been paid back, it still leaves a lot of people wary of the same thing happening again.

- **The Debate on Bitcoin Scalability**

The cryptocurrency community is up in arms over how the blockchain will be upgraded for future users. As the time and fees required for verifying a transaction climbs to record highs, more businesses are having a tough time accepting Bitcoins for payment. In early 2017, more than 50 companies came together to speed up transactions, but till now the results have not yet been felt. As a result, more users might start using normal modes of currency to overcome such blockchain hassles.

- **The Rise of the Rivals**

Today, Bitcoin is not the only game in town, and while its value has increased by almost 100% since the beginning of 2016, its share of the digital currency pile is rapidly reducing owing to almost 700 different competitors. Its market share has reduced to 50% from 85% a year before, a sign of the times to come.

- **Unrecognized by Governments**

Most of the general populace doesn't understand Bitcoins, and nor does most of the world's governments. The cost of gaining a license to set up cryptocurrency companies is sky-high, and there are no regulations in sight which might make it easier for people looking to invest into them. The U.S. Securities and Exchange Commission recently rejected a proposal by Bitcoin to run a publicly traded fund based on the digital currency, which in turn led to a big plummet in Bitcoin's shares. ▶

SUPPORT THE CAMPAIGN



LOOK OUT FOR THE RED LINE

BE RESPONSIBLE

Medicines such as Antibiotics have a Red Vertical Line on their pack to indicate that these should be consumed only on doctor's prescription. Always complete the full course as prescribed by the doctor.

SIGN THE PLEDGE.

[HTTP://WWW.CAUSES.COM/CAMPAIGNS/106670-RAISE-AWARENESS-FOR-SALE-USE-OF-ANTIBIOTICS-TO-COMBAT-AMR](http://www.causes.com/campaigns/106670-RAISE-AWARENESS-FOR-SALE-USE-OF-ANTIBIOTICS-TO-COMBAT-AMR)

Campaign Partners



French Company Launches Heater Which **Warms The Room** while Mining Cryptocurrencies



The company, along with the heater, also provides a smartphone app which keeps track of the cryptocurrencies mined by the device as well as the market

WITH AN AIM to 'make heating a source of revenue, not an expense', a French technology company has launched a crypto heater — a room heating device which uses the heat dissipated by (included) GPUs while mining cryptocurrencies to warm a room.

The crypto heater QC-1 by Qarnot, a cuboid-shape aluminum and wood device packs 2 GPUs Nitro+ Radeon RX 580 8G which gives an output at 60 Megahash (MH) per second. The computing power from the GPUs is used for mining cryptocurrencies.

The heater has two heating modes—mining mode and booster mode—former to be used normally and latter to be used when there is extreme cold. In the mining mode, the power used by the device is 450 Watts whereas, in the booster mode, two embedded resistors start working, taking the energy consumption to 650 Watts and providing extra heat.

"We estimate that a QC1 can heat a 20 sqm room. Isolation, ceiling height are obviously to take into consideration

as well. QC-1 generates a high-quality soft heat: you need less power than with a more "classic" electricity heater," the company says.

The company, along with the heater, also provides a smartphone app which keeps track of the cryptocurrencies mined by the device as well as the market.

Currently, the device is pre-set to mine the most profitable of the top three cryptocurrencies but the company promises to provide updates to adapt it to mine any currency in future.

The company claims that the device is mining ready and it would take just 10 minutes to install for a user. All it needs is an electric socket to plug in the device and internet connection.

The QC-1 is priced at EUR 2900 (approx. Rs 2.32 lakh) and the company promises to ship it to anywhere in the world. The delivery of product will begin from June 20, however, pre-booking is open as of now. ▶

CONSUMERS, BEWARE



No Matter How Deep Your Knowledge Base, Only Use The Money You Can Afford To Lose When Speculating In Cryptocurrencies

Risks to consider: Cryptocurrency investing is uncharted territory. While we are certain we are in the midst of radical economic changes, no one knows for certain which cryptocurrencies will survive long term.

Think about the dot-com boom: Many companies folded but a few survived creating extreme wealth for their early investors. The same thing will likely happen in the crypto space.

CRYPTOCURRENCIES HAVE BEEN

compared to ponzi schemes, pyramid schemes and economic bubbles, such as housing market bubbles. Howard Marks of Oaktree Capital Management stated in 2017 that digital currencies were "nothing but an unfounded fad (or perhaps even a pyramid scheme), based on a willingness to ascribe value to something that has little or none beyond what people will pay for it", and compared them to the tulip mania (1637), South Sea Bubble (1720), and dot-com bubble (1999). In October 2017, BlackRock CEO Larry Fink called bitcoin an 'index of money laundering'. "Bitcoin just shows you how much demand for money laundering there is in the world," he said.

While cryptocurrencies are digital currencies that are managed through advanced encryption techniques, many governments have taken a cautious approach toward them, fearing their lack of central control and the effects they could have on financial security. Regulators in

several countries have warned against cryptocurrency and some have taken concrete regulatory measures to dissuade users. Additionally, many banks do not offer services for cryptocurrencies and can refuse to offer services to virtual-currency companies. While traditional financial products have strong consumer protections in place, there is no intermediary with the power to limit consumer losses if bitcoins are lost or stolen. One of the features cryptocurrency lacks in comparison to credit cards, for example, is consumer protection against fraud, such as chargebacks.

An enormous amount of energy goes into proof-of-work cryptocurrency mining, although cryptocurrency proponents claim it is important to compare it to the consumption of the traditional financial system.

There are also purely technical elements to consider. For example, technological advancement in cryptocurrencies such as bitcoin result in high up-front costs to miners in the form of specialized hardware and

software. Cryptocurrency transactions are normally irreversible after a number of blocks confirm the transaction. Additionally, cryptocurrency can be permanently lost from local storage due to malware or data loss. This can also happen through the destruction of the physical media, effectively removing lost cryptocurrencies forever from their markets.

The cryptocurrency community refers to pre-mining, hidden launches, ICO or extreme rewards for the altcoin founders as a deceptive practice. It can also be used as an inherent part of a cryptocurrency's design. Pre-mining means currency is generated by the currency's founders prior to being released to the public.

Paul Krugman, Nobel Memorial Prize in Economic Sciences winner does not like bitcoin, has repeated numerous times that it is a bubble that will not last and links it to Tulip mania.

American business magnate Warren Buffett thinks that cryptocurrency will come to a bad ending.



consumers, beware

NO MATTER HOW DEEP YOUR KNOWLEDGE BASE ...



LOSS.THEFT.FRAUD.

GBL, a Chinese bitcoin trading platform, suddenly shut down on Oct. 26, 2013. Subscribers, unable to log in, lost up to \$5 million worth of bitcoin.

In February 2014, cryptocurrency made headlines due to the world's largest bitcoin exchange, Mt. Gox, declaring bankruptcy. The company stated that it had lost nearly \$473 million of their customer's bitcoins likely due to theft. This was equivalent to approximately 750,000 bitcoins, or about 7% of all the bitcoins in existence. Due to this crisis, among other news, the price of a bitcoin fell from a high of about \$1,160 in December to under \$400 in February.

Two members of the Silk Road Task Force—a multi-agency federal task force that carried out the U.S. investigation of Silk Road—seized bitcoins for their own use in the course of the investigation. DEA agent Carl Mark Force IV, who attempted to extort Silk Road founder Ross Ulbricht ("Dread Pirate Roberts"), pleaded guilty to money laundering, obstruction of justice, and extortion under color of official right, and was sentenced to 6.5 years in federal prison. U.S. Secret Service agent Shaun Bridges

The U.S. Securities and Exchange Commission separately brought a civil enforcement action against Garza, who was eventually ordered to pay a judgment of \$9.1 million plus \$700,000 in interest.

pleaded guilty to crimes relating to his diversion of \$800,000 worth of bitcoins to his personal account during the investigation, and also separately pleaded guilty to money laundering in connection with another cryptocurrency theft; he was sentenced to nearly eight years in federal prison.

Homero Josh Garza, who founded the cryptocurrency startups GAW Miners and ZenMiner in 2014, acknowledged in a plea agreement that the companies were part of a pyramid scheme, and pleaded guilty to wire fraud in 2015. The U.S. Securities and Exchange Commission separately brought a civil enforcement action against Garza, who was eventually ordered to pay a judgment of \$9.1 million

plus \$700,000 in interest. The SEC's complaint stated that Garza, through his companies, had fraudulently sold "investment contracts representing shares in the profits they claimed would be generated" from mining.

On November 21, 2017, the Tether cryptocurrency announced they were hacked, losing \$31 million in USD from their primary wallet. The company has 'tagged' the stolen currency, hoping to 'lock' them in the hacker's wallet (making them unspendable). Tether indicates that it is building a new core for its primary wallet in response to the attack in order to prevent the stolen coins from being used.

On December 6, 2017, more than \$60 million worth of bitcoin was stolen after a cyber attack hit the cryptocurrency mining platform NiceHash (Slovenia-based company). According to the CEO Marko Kobal and co-founder Sasa Coh, bitcoin worth \$64 million USD was stolen, although users have pointed to a bitcoin wallet which holds 4,736.42 bitcoins, equivalent to \$67 million. ▀

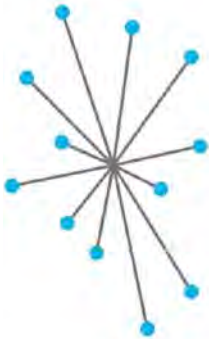
All About Cryptocurrency



What Is a Cryptocurrency?

A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets.

Centralized



Decentralized



Distributed Ledgers



The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous

- Each user has a copy of the ledger and participates in confirming transactions independently

- Users (●) are not anonymous

- Permission is required for users to have a copy of the ledger and participate in confirming transactions

CRYPTOCURRENCIES ARE A type of digital currencies, alternative currencies and virtual currencies.

Cryptocurrencies use decentralized control as opposed to centralized electronic money and central banking systems. The decentralized control of each cryptocurrency works through a blockchain, which is a public transaction database, functioning as a distributed ledger.

Bitcoin, created in 2009, was the first decentralized cryptocurrency. Since then, numerous other cryptocurrencies have been created. These are frequently called altcoins, as a blend of alternative coin.

Cryptocurrency is designed from the ground up to take advantage of the internet and how it works. Instead of relying on traditional financial institutions who verify and guarantee your transactions, cryptocurrency transactions are verified by the user's computers logged into the currency's network. Since the currency is protected and encrypted, it becomes impossible to increase the money supply over a predefined algorithmic rate. All users are aware of the algorithmic rate. Therefore, since each algorithm has a roof limit, no cryptocurrency can be produced or "mined" beyond that.

Since Cryptocurrency is completely in the cloud, it does not attain a physical form but have a digital value, and can be used for digital equivalent of cash in a steadily increasing number of retailers and other businesses. While there is a small fee for every cryptocurrency transaction, it is still considerably lesser than the usual credit card processing fees.

A cryptocurrency is a system that meets all of the following six conditions:

- 1 The system does not require a central authority, distributed achieve consensus on its state.
- 2 The system keeps an overview of cryptocurrency units and their ownership.
- 3 The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
- 4 Ownership of cryptocurrency units can be proved exclusively cryptographically.
- 5 The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
- 6 If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

In March 2018, the word "cryptocurrency" was added to the Merriam-Webster Dictionary.

BREAKING DOWN 'Cryptocurrency'

The anonymous nature of cryptocurrency transactions makes them well-suited for a host of nefarious activities,

such as money laundering and tax evasion. The first cryptocurrency to capture the public imagination was Bitcoin, which was launched in 2009.

Decentralized cryptocurrency is produced by the entire cryptocurrency system collectively, at a rate which is defined when the system is created and which is publicly known. In centralized banking and economic systems such as the Federal Reserve System, corporate boards or governments control the supply of currency by printing units of fiat money or demanding additions to digital banking ledgers. In case of decentralized cryptocurrency, companies or governments cannot produce new units, and have not so far provided backing for other firms, banks or corporate entities which hold asset value measured in it. As of September 2015, there were over 14.6 million bitcoins in circulation with a total market value of \$3.4 billion. Bitcoin's success has spawned a number of competing cryptocurrencies, such as Litecoin, Namecoin and PPCoin, most are similar to and derive from the first fully implemented decentralized cryptocurrency, bitcoin. Within cryptocurrency systems the safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners: members of the general public using their computers to help validate and timestamp transactions, adding them to the ledger in accordance with a particular timestamping scheme. Miners have a financial incentive to maintain the security of a cryptocurrency ledger.

Most cryptocurrencies are designed to gradually decrease production of currency, placing an ultimate cap on the total amount of currency that will ever be in circulation, mimicking precious metals. Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies can be more difficult for seizure by law enforcement. This difficulty is derived from leveraging cryptographic technologies.

MINING

Ever wondered how bitcoins are actually made?

Over the past several years, cryptocurrencies like Bitcoin have been quietly growing in popularity, with an ever-larger number of people buying and selling them. Now that Bitcoin has hit the mainstream and become a worldwide phenomenon, more people than ever are looking to get into the cryptocurrency game.

However, the production of cryptocurrencies isn't anything like that of regular money. There's no central

authority that issues new notes; instead, bitcoins (or litecoins, or any of the other so-called 'alt-coins') are generated through a process known as 'mining'. So what is cryptocurrency mining, and how does it work?

Cryptocurrency Mining and Blockchains

Before getting to grips with the process of cryptocurrency mining, we need to first understand what a blockchain is and how that works. Blockchain is a technology that supports almost every cryptocurrency. It is a public ledger (decentralised register) of every transaction that has been carried out in that cryptocurrency.

These transactions are assembled into what are called "blocks". These are the verified to ensure they are legitimate by cryptocurrency miners. This checks if the same coin hasn't been expended again before the transaction has cleared, and that the input and output expenses tally. Then the next sequential transaction block is connected to it. This is how cryptocurrencies are created and how new cryptocurrencies are made.

The block time is the average time it takes for the network to generate one extra block in the blockchain. Some blockchains create a new block as frequently as every five seconds. By the time of block completion, the included data becomes verifiable. This is practically when the money transaction takes place, so a shorter block time means faster transactions.

By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin, the tech community is now finding other potential uses for the technology.

A distributed database

Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain.

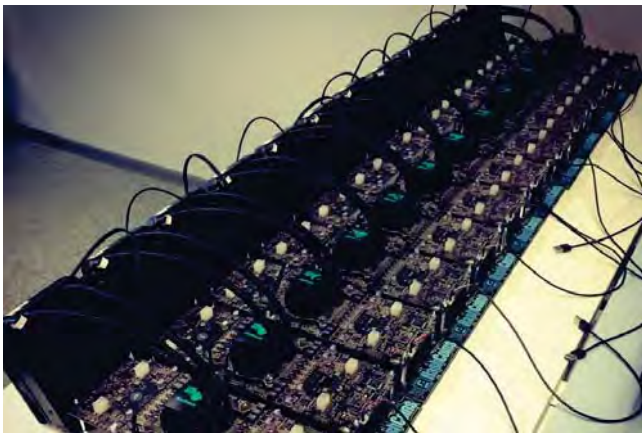
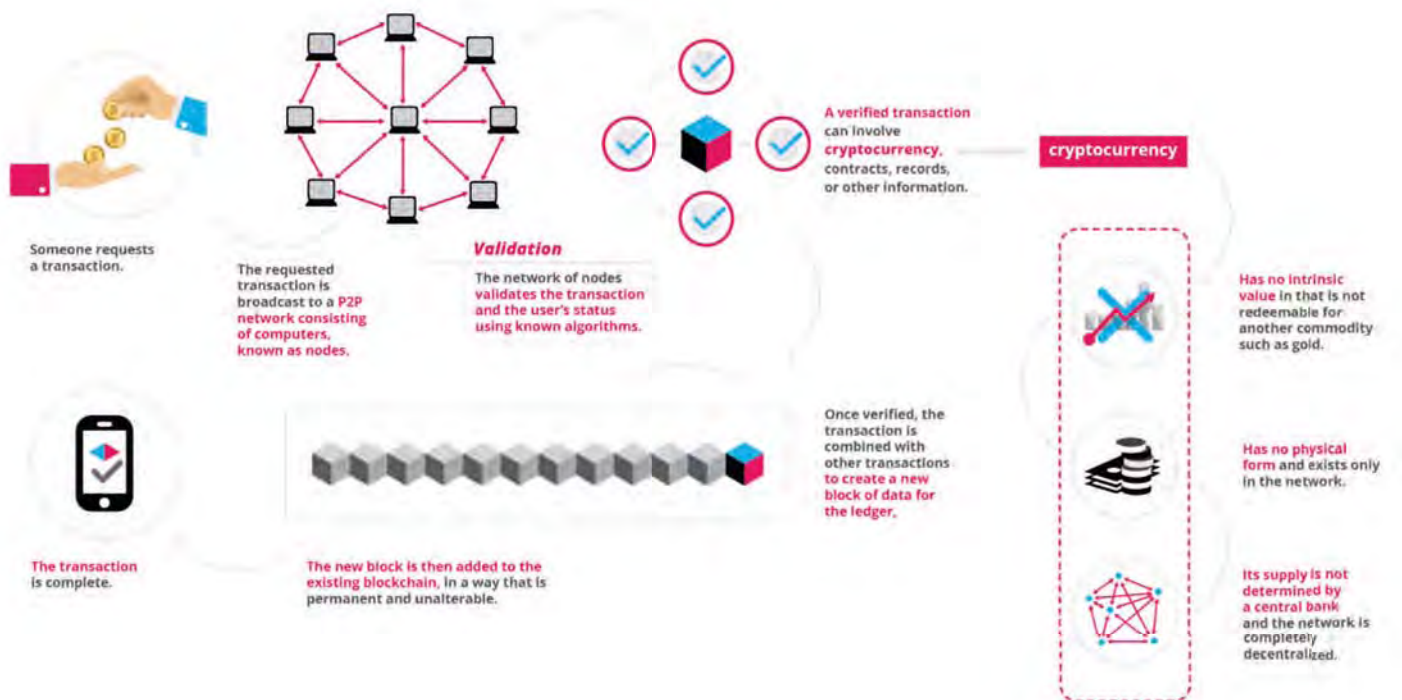
Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

Blockchain Durability and robustness

Blockchain technology is like the internet in that it has a built-in robustness. By storing blocks of information that are identical across its network, the blockchain cannot:

- 1 Be controlled by any single entity.
- 2 Has no single point of failure





Mining new blocks

As there is no central authority or central bank, there has to be a way of gathering every transaction carried out with a cryptocurrency in order to create a new block. Network nodes that carry out this task called 'miners'. Every time a slew of transactions is amassed into a block, this is appended to the blockchain. Whoever appends the block gets rewarded with some of that cryptocurrency.

To prevent the devaluation of the currency by miners building lots of blocks, the task is made harder to conduct. This is achieved by making miners solve complicated mathematical problems called 'proof of work'.

Calculating hashes

In order to successfully create a block, it must be accompanied by a cryptographic hash that fulfills certain

requirements. The only feasible way to arrive at a hash matching the correct criteria is to simply calculate as many as possible and wait until you get a matching hash. When the right hash is found, a new block is formed and the miner that found it is awarded with units of cryptocurrency.

Think of it like one of those competitions where you have to guess the weight of the cake - only you get unlimited guesses, and the first one to submit a correct answer wins. Whoever can make guesses at the fastest rate has a higher chance of winning.

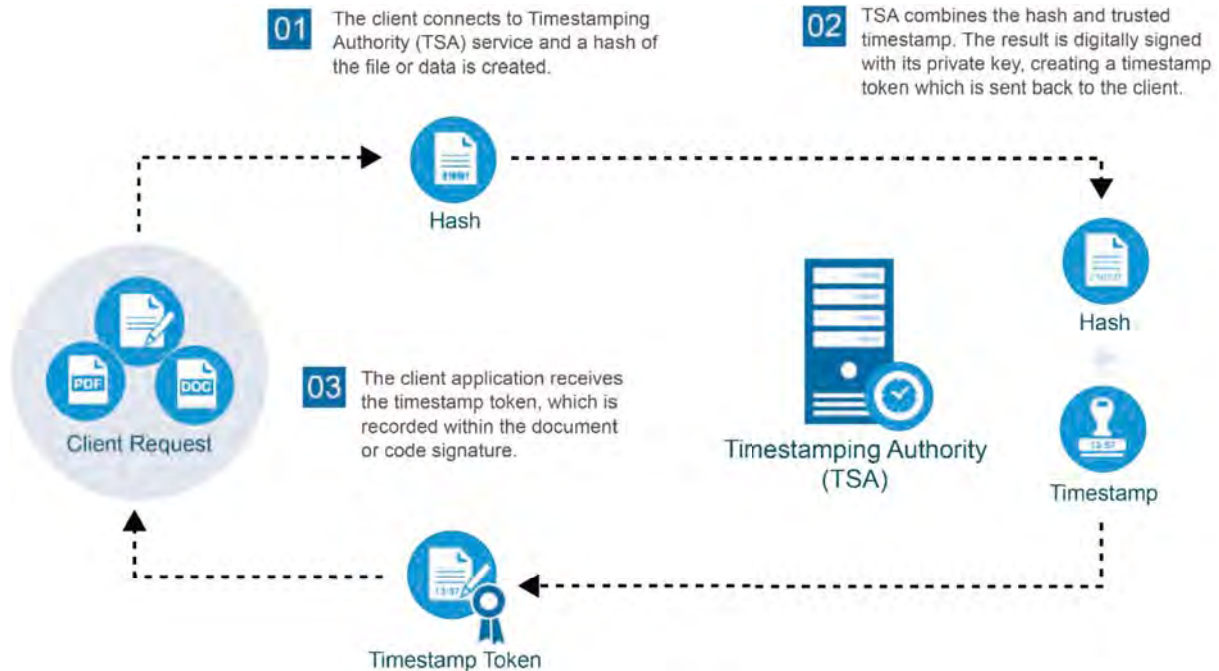
Cryptocurrency mining limits

In practice, this means that miners are competing against each other to calculate as many hashes as possible, in the hopes of getting to be the first one to hit the correct one, form a block and get their cryptocurrency payout.

However, the difficulty of calculating the hashes also scales - every new block of bitcoins becomes harder to mine. In theory, this ensures that the rate at which new blocks are created remains steady. Many cryptocurrencies also have a finite limit on the amount of units that can ever be generated. For example, there will only ever be 21 million Bitcoins in the world. After that, mining a new block will not generate any bitcoins at all.

Cryptocurrency mining requirements

While it used to be possible to mine your own cryptocurrencies using a regular PC, for the most part that is no longer the case. As more people start mining, the hardware necessary to mine effectively increases; from a moderately-powerful processor, to a high-end



GPU, to several GPUs working together, to specialised chips designed specifically for mining.

In order to successfully mine most modern cryptocurrencies, you'll need to spend at least £1,000 on hardware, as well as footing the substantial electricity bill that having it running 24/7 will generate. In fact, most miners spend the vast majority of their mining income on covering the costs of running their equipment.

Now that the Bitcoin boom is thoroughly underway, certain companies and groups have started putting serious money behind it, with large warehouses full of floor-to-ceiling racks of expensive graphics cards, doing nothing but trying to mine new units of Bitcoin, Litecoin, Ether and the like.

For context, the Bitcoin network processes 5.5 quintillion hashes per second. Unless you have equipment that can process a vast number of calculations in a very short space of time, your odds of competing with large mining operations are infinitesimally small. This is why many miners join forces, banding together to create 'mining pools', sharing their compute power and any returns generated from their efforts.

Given the economic and environmental concerns associated with mining, various "minerless" cryptocurrencies are undergoing active development. Unlike conventional blockchains, some directed acyclic graph cryptocurrencies utilise a pay-it-forward system, whereby each account performs minimally heavy computations on two previous transactions to verify. Other cryptocurrencies like Nano utilise a block-lattice structure whereby each individual account has its own blockchain. With each account controlling its own transactions, no traditional proof-of-work mining is required, allowing for free, instantaneous transactions.

TIMESTAMPING

Cryptocurrencies use various time stamping schemes to avoid the need for a trusted third party to timestamp transactions added to the blockchain ledger.

What is Timestamping?

When the date and time of an event is recorded, we say that it is timestamped. A digital camera will record the time and date of a photo being taken, a computer will record the time and date of a document being saved and edited. A social media post may have date and time recorded. These are all examples of a timestamp.

Timestamps are important for keeping records of when information is being exchanged or created or deleted online. In many cases, these records are simply useful for us to know about. But in some cases, a timestamp is more valuable.

Imagine this scenario: your organization electronically signs a legal agreement or NDA with another organization or contractor. Later down the line, it is discovered that the contractor has leaked information about the project under which the NDA was signed. The contractor disputes the NDA, arguing that information was shared prior to the signing of the NDA. Knowing when that document was actually signed is essential here.

In a legal setting like this, it's not enough to just have a timestamp. If your argument comes down to when the NDA was signed, you need to be able to prove that the timestamp of the signature is valid, that it says the document was signed when it was actually

India Customs Govt Refuses Importing Cryptocurrency Mining Machines

signed. Timestamps that rely on system clocks are not enough, since it's not difficult to alter the date and time locally on a machine. Plus, there are a variety of tools online that will allow you to change the modified, created and last accessed date of a document or PDF. So, how do we know if we can trust the timestamp?

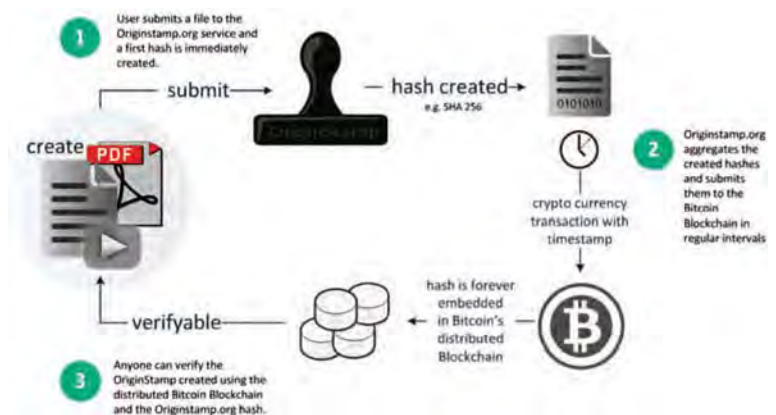
What is a Trusted Timestamp?

This is where 'trusted' timestamping comes in. These types of timestamps are generated by a trusted third party using secure FIPS-compliant hardware, so they are not subject to manipulation by a local user. Trusted timestamping means that you can say with a high level of certainty that the date on the timestamp is accurate and hasn't been tampered with.

How Does Timestamping Work?

Timestamping Authorities (TSAs) use Public Key Infrastructure (PKI) technology to apply timestamps. Here is a high level summary of the steps involved.

- 1 The client application creates a hashed value (as a unique identifier of the data or file that needs to be timestamped) and sends it to the TSA.
- 2 From now on, any change (even by a single bit of information) in the original file will require communication of changes with the TSA server.
- 3 The TSA combines the hash and other information, including the authoritative time. The result is digitally



signed with the TSA's private key, creating a timestamp token which is sent back to the client. The timestamp token contains the information the client application will need to verify the timestamp later.

- 4 The timestamp token is received by the client application and recorded within the document or code signature.

When the resulting timestamped data or file is opened in the future, the client application will use the TSA's public key to authenticate the TSA (i.e. validate that the timestamp came from a trusted TSA) and re-calculate a hash of the original data. This new hash is compared to the originally created hash (step 1 above). If any changes have been made to the data since the timestamp was applied, this hash check will fail and warning messages will be shown saying that the data has been altered and it should not be trusted. 📌

Cryptocurrencies: Dawn of a new economy

US mobile payments are expected to hit \$142 billion by 2019



"Peer-to-peer" transfer occur when one person pays another person using a mobile device. The device uses either a preloaded app or a browser-based app to initiate, authenticate, and transfer funds

Peer-to-peer



"In-person" purchases are initiated using a mobile device where the buyer and seller are in-person, usually at a brick-and-mortar retail location where the product/ service is immediately delivered.

In-person



"Remote" payments are made when a buyer purchases goods or services using a mobile device, but the buyer is not physically present with the seller and the good are not immediately delivered (as with eCommerce).

Remote

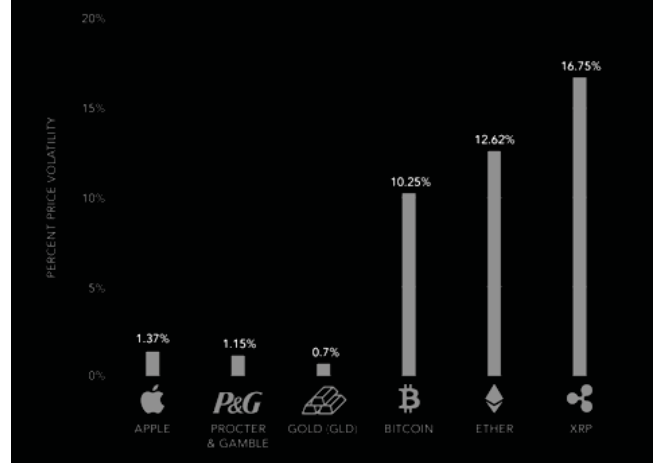
MOSTLY DUE TO its revolutionary properties cryptocurrencies have become a success their inventor, Satoshi Nakamoto, didn't dare to dream of. While every other attempt to create a digital cash system didn't attract a critical mass of users, Bitcoin had something that provoked enthusiasm and fascination. Sometimes it feels more like religion than technology.

Cryptocurrencies are digital gold. Sound money that is secure from political influence. Money that promises to preserve and increase its value over time. Cryptocurrencies are also a fast and comfortable means of payment with a worldwide scope, and they are private and anonymous enough to serve as a means of payment for black markets and any other outlawed economic activity.

But while cryptocurrencies are more used for payment, its use as a means of speculation and a store of value dwarfs the payment aspects. Cryptocurrencies gave birth to an incredibly dynamic, fast-growing market for investors and speculators. Exchanges like Okcoin, poloniex or shapeshift enables the trade of hundreds of cryptocurrencies. Their daily trade volume exceeds that of major European stock exchanges.





















At the same time, the praxis of Initial Coin Distribution (ICO), mostly facilitated by Ethereum's smart contracts, gave life to incredibly successful crowdfunding projects, in which often an idea is enough to collect millions of dollars. In the case of "The Decentralized Autonomous Organisation (DAO)" it has been more than 150 million dollars.

Average Daily Price Volatility (January 2018)



In this rich ecosystem of coins and token, you experience extreme volatility. It's common that a coin gains 10 percent a day – sometimes 100 percent – just to lose the same at the next day. If you are lucky, your coin's value grows up to 1000 percent in one or two weeks.

While Bitcoin remains by far the most famous cryptocurrency and most other cryptocurrencies have zero non-speculative impact, investors and users should keep an eye on several cryptocurrencies. Here we present the most popular cryptocurrencies of today.

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$11,382,240,050	\$712.76	15,969,336 BTC	\$67,288,200	-1.60%	
2	 Ethereum	\$904,848,975	\$10.54	85,831,133 ETH	\$4,069,260	-1.21%	
3	 Ripple	\$290,446,848	\$0.008121	35,765,131,899 XRP *	\$2,386,420	0.26%	
4	 Litecoin	\$184,904,214	\$3.82	48,378,029 LTC	\$2,258,970	-1.05%	
5	 Monero	\$83,466,495	\$6.27	13,311,446 XMR	\$3,134,490	5.38%	
6	 Ethereum Classic	\$80,817,441	\$0.942637	85,735,486 ETC	\$603,573	2.21%	
7	 Dash	\$66,519,213	\$9.68	6,874,532 DASH	\$596,632	-0.77%	
8	 Augur	\$52,038,360	\$4.73	11,000,000 REP *	\$396,072	6.38%	
9	 NEM	\$37,322,550	\$0.004147	8,999,999,999 XEM *	\$86,817	4.40%	
10	 Waves	\$35,727,500	\$0.357275	100,000,000 WAVES *	\$133,650	-3.94%	

Source: coinmarketcap

Types of Cryptocurrencies

A Guide To Today's Cryptocurrencies

The huge run-up in bitcoin, ether, ripple, and others has focused the public's attention on the rapidly expanding world of cryptocurrencies.

People from every walk of life are jumping in and taking speculative risks on certain cryptocurrencies. Stories abound of folks buying a few hundred coins for under a thousand dollars, forgetting about them, and then being pleasantly surprised when their coins are worth millions a few years later.

Most of these winning investors are simply lucky -- a long shot speculation that paid off hugely.

At the same time, many others have made fortunes by building knowledge about the blockchain and cryptocurrencies. Knowledge, like with traditional investments, is the key to creating consistent profits in the new world of digital assets. When you understand the basics of how blockchain technology and cryptocurrencies work, it becomes easier to make intelligent decisions about investing.

Each cryptocurrency solves a particular problem and fits into one of three categories. These categories are transactional, platform, and utility. It is important to note that some cryptocurrencies can fit into more than one category.

Let's take a closer look at each of these categories and examples of each.

1. Transactional

This is the original category for cryptocurrencies. Transactional cryptocurrencies are designed to be used as money and exchanged for goods and services. Bitcoin, litecoin, and a host of others are transactional cryptocurrencies.

Transactional cryptocurrencies are intended to eliminate the need for government-issued currency. Indeed, some form of cryptocurrency will likely replace all fiat currency one day. But the replacement cryptos may still come from central banks -- Singapore's government, for one, is testing out this idea with its Project Ubin.

2. Platform

Platform cryptocurrencies are designed to eliminate middlemen, create markets, and even launch other cryptocurrencies. Platform cryptocurrencies provide the backbone for a host of future applications.

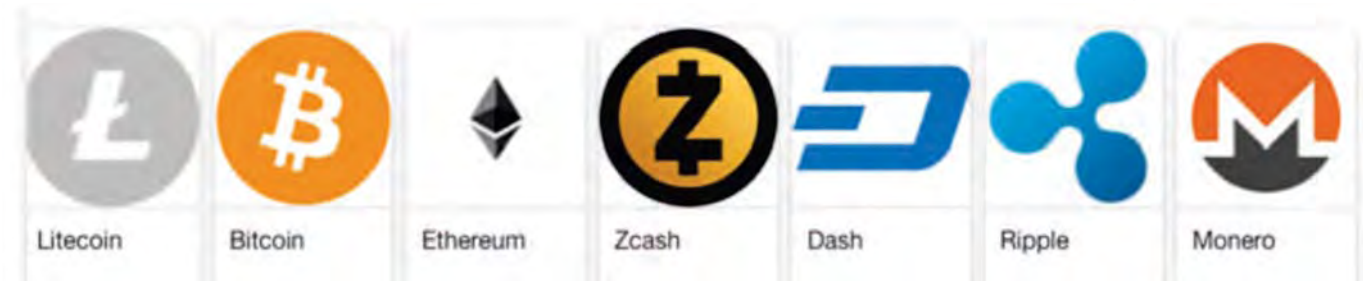
Ethereum is a prime example of a platform cryptocurrency. Ethereum is a decentralized platform that is used to run smart contracts. A smart contract is an application that runs exactly as programmed without the possibility of fraud, censorship, or even downtime.

Ethereum is also the building block of many of the new cryptocurrencies.

3. Utility

A utility cryptocurrency is designed for a particular task. Ripple (XRP) is an example of a utility cryptocurrency. Designed to facilitate fiat money transfer in an economical and highly efficient manner, ripple is used by multiple banks and institutions. Some of the names on their website include UBS, Santander, BMO and American Express.

The 6 Most Important Cryptocurrencies Other Than Bitcoin



Bitcoin

Bitcoin has not just been a trendsetter, ushering in a wave of cryptocurrencies built on decentralized peer-to-peer network, it's become the de facto standard for cryptocurrencies. The one and only, the first and most famous cryptocurrency. Bitcoin serves as a digital gold standard in the whole cryptocurrency-industry, is used as a global means of payment and is the de-facto currency of cyber-crime like darknet markets or ransomware. After seven years in existence, Bitcoin's price has increased from zero to more than 650 Dollar, and its transaction volume reached more than 200.000 daily transactions.

There is not much more to say: Bitcoin is here to stay.

Other Important Cryptocurrencies

The currencies inspired by Bitcoin are collectively called altcoins and have tried to present themselves as modified or improved versions of Bitcoin. While some of these currencies are easier to mine than Bitcoin is, there are tradeoffs, including greater risk brought on by lesser liquidity, acceptance and value retention. Since Bitcoin prices are soaring new highs, we look at six cryptocurrencies, picked from over 700 (in no specific order) that could be worth your while.

1) Litecoin (LTC)

Litecoin, launched in the year 2011, was among the initial cryptocurrencies following bitcoin and was often referred to as 'silver to Bitcoin's gold.' It was created by Charlie Lee, a MIT graduate and former Google engineer. Litecoin is based on an open source global payment network that is not controlled by any central authority and uses "scrypt" as a proof of work, which can be decoded with the help of CPUs of consumer grade. Although

Litecoin is like Bitcoin in many ways, it has a faster block generation rate and hence offers a faster transaction confirmation. Other than developers, there are a growing number of merchants who accept Litecoin.

Litecoin was a real innovation, perfectly tailored to be the smaller brother of bitcoin. "It facilitated the emerge of several other cryptocurrencies which used its codebase but made it, even more, lighter". Examples are Dogecoin or Feathercoin.

While Litecoin failed to find a real use case and lost its second place after bitcoin, it is still actively developed and traded and is hoarded as a backup if Bitcoin fails.

2) Ethereum (ETH)

The brainchild of young crypto-genius Vitalik Buterin has ascended to the second place in the hierarchy of cryptocurrencies. Launched in 2015, Ethereum is a decentralized software platform that enables Smart Contracts and Distributed Applications (DApps) to be built and run without any downtime, fraud, control or interference from a third party. During 2014, Ethereum had launched a pre-sale for ether which had received an overwhelming response. The applications on Ethereum are run on its platform-specific cryptographic token, ether. Ether is like a vehicle for moving around on the Ethereum platform, and is sought by mostly developers looking to develop and run applications inside Ethereum. According to Ethereum, it can be used to "codify, decentralize, secure and trade just about anything." After the Hack of the DAO in 2016 – an Ethereum based smart contract – the developers decided to do a hard fork without consensus, which resulted in the emerge of Ethereum Classic (ETC). Besides this, there are several clones of Ethereum, and Ethereum itself is a host of several Tokens like DigixDAO and Augur. This makes Ethereum more a family of cryptocurrencies than a single currency. Ethereum (ETH) has a market capitalization of \$41.4 billion.

3) Zcash (ZEC)

Zcash, a decentralized and open-source cryptocurrency launched in the latter part of 2016, looks promising. "If Bitcoin is like http for money, Zcash is https," is how Zcash defines itself. Zcash offers privacy and selective transparency of transactions. Thus, like https, Zcash claims to provide extra security or privacy where all transactions are recorded and published on a blockchain, but details such as the sender, recipient, and amount

remain private. Zcash offers its users the choice of 'shielded' transactions, which allow for content to be encrypted using advanced cryptographic technique or zero-knowledge proof construction called a zk-SNARK developed by its team.

4) Dash

Dash (originally known as Darkcoin) is a more secretive version of Bitcoin. Dash offers more anonymity as it works on a decentralized mastercode network that makes transactions almost untraceably. Launched in January 2014, Dash experienced an increasing fan following in a short span of time. This cryptocurrency was created and developed by Evan Duffield and can be mined using a CPU or GPU. In March 2015, 'Darkcoin' was rebranded to Dash, which stands for Digital Cash and operates under the ticker – DASH. The rebranding didn't change any of its technological features such as Darksend, InstantX.

5) Ripple (XRP)

Maybe the less popular or most hated project in the cryptocurrency community is Ripple.

Ripple is a real-time global settlement network that offers instant, certain and low-cost international payments. Ripple "enables banks to settle cross-border payments in real time, with end-to-end transparency, and at lower costs." Released in 2012, Ripple currency has a market capitalization of \$1.26 billion. Ripple's consensus ledger -- its method of conformation -- doesn't need mining, a feature that deviates from bitcoin and altcoins. Since Ripple's structure doesn't require mining, it reduces the usage of computing power, and minimizes network latency. Ripple believes that 'distributing value is a powerful way to incentivize certain behaviors' and thus currently plans to distribute XRP primarily "through business development deals, incentives to liquidity providers who offer tighter spreads for payments, and selling XRP to institutional buyers interested in investing in XRP."

While Ripple has a native cryptocurrency, XRP, it is more about a network to process IOUs than the cryptocurrency itself. XRP, the currency, doesn't serve as a medium to store and exchange value, but more as a token to protect the network against spam.

Ripple Labs created every XRP-token, the company running the Ripple network, and is distributed by them on will. For this reason, Ripple is often called pre-mined in the community and dissed as no real cryptocurrency, and XRP is not considered as a good store of value.

Banks, however, seem to like Ripple. At least they adopt the system with an increasing pace.

6) Monero (XMR)

Monero is a secure, private and untraceable currency. This open source cryptocurrency was launched in April 2014 and soon spiked great interest among the

cryptography community and enthusiasts. The development of this cryptocurrency is completely donation-based and community-driven. Monero has been launched with a strong focus on decentralization and scalability, and enables complete privacy by using a special technique called 'ring signatures.' With this technique, there appears a group of cryptographic signatures including at least one real participant – but since they all appear valid, the real one cannot be isolated.

Monero is the most prominent example of the cryptonite algorithm. This algorithm was invented to add the privacy features Bitcoin is missing. If you use Bitcoin, every transaction is documented in the blockchain and the trail of transactions can be followed. With the introduction of a concept called ring-signatures, the cryptonite algorithm was able to cut through that trail.

The first implementation of cryptonite, Bytecoin, was heavily premined and thus rejected by the community. Monero was the first non-premined clone of bytecoin and raised a lot of awareness. There are several other incarnations of cryptonote with their own little improvements, but none of it did ever achieve the same popularity as Monero.

'Moneros popularity peaked in summer 2016 when some darknetmarkets decided to accept it as a currency. This resulted in a steady increase in the price, while the actual usage of Monero seems to remain disappointingly small.

The Bottom Line

Bitcoin continues to lead the pack of cryptocurrencies, in terms of market capitalization, user base and popularity. Nevertheless, virtual currencies such as Ethereum and Ripple which are being used more for enterprise solutions are becoming popular, while some altcoins are being endorsed for superior or advanced features vis-à-vis Bitcoins. Besides these, there are hundreds of cryptocurrencies of several families. Most of them are nothing more than attempts to reach investors and quickly make money, but a lot of them promise playgrounds to test innovations in cryptocurrency-technology.

Going by the current trend, cryptocurrencies are here to stay but how many of them will emerge leaders amid the growing competition within the space will only be revealed with time.

List of Cryptocurrencies

The number of cryptocurrencies available over the internet as of 7 January 2018 is over 1384 and growing. A new cryptocurrency can be created at any time. By market capitalization, Bitcoin is currently (January 6, 2018) the largest blockchain network, followed by Ethereum, Ripple, Bitcoin Cash, Cardano, and Litecoin.

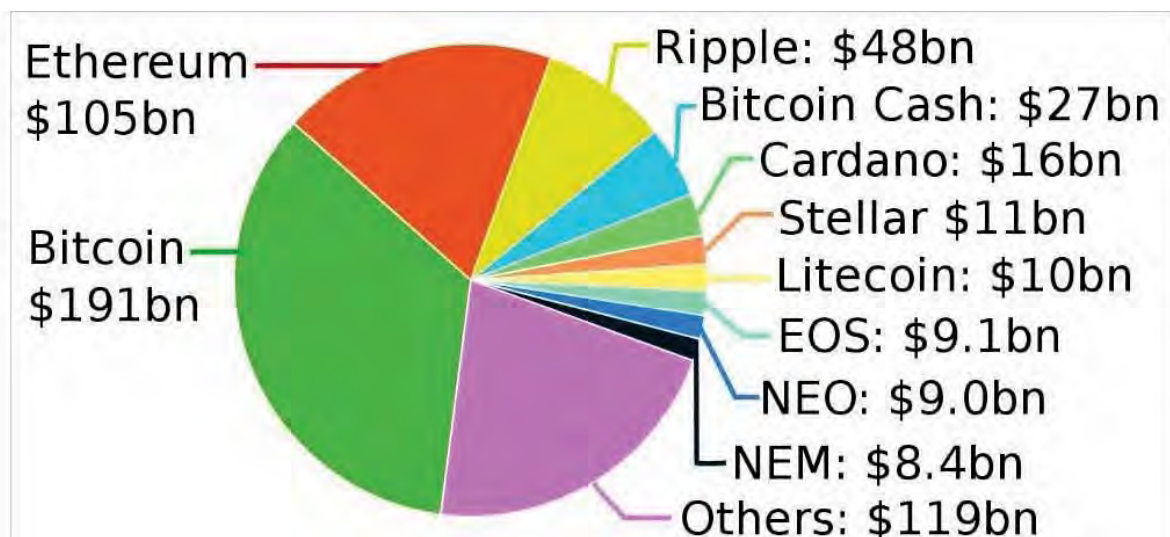
Cryptocurrencies

Release	Status	Currency	Symbol	Founder(s)	Hash algorithm	Programming language of implementation blockchain	Crypto-currency (PoS, PoW, or other)	Notes
2009	Active	Bitcoin	BTC, XBT,	Satoshi Nakamoto [nt 1]	SHA-256d [6][7]	C++[8]	PoW[7][9]	The first decentralized ledger currency. Cryptocurrency with the most famous, popular, notable and highest market capitalization.
2011	Active	Litecoin	LTC, Ł	Charlie Lee	Script	C++[10]	PoW	The first cryptocurrency to use Script as a hashing algorithm.
2011	Active	Namecoin	NMC	Vincent Durham [11][12]	SHA-256d	C++[13]	PoW	Also acts as an alternative, decentralized DNS.
2011	Active	Swift Coin	STC	Daniel Bruno	SHA-256		PoW	First digital coin with theoretical value based on the work required to produce electricity. First block chain to support currency creation by interest paid on debt. Solidus Bond proto smart-contract. One of the first digital coins patented in the US. First block chain to support encrypted mail with attachments.
2012	Active	Bytecoin	BCN		Crypto Note	C++[14]	PoW	First cryptocurrency based on the Crypto Note algorithm. Focused on user privacy through impassive and anonymous transactions
2012	Active	Peercoin	PPC	Sunny King (pseudo-nym)[15]	SHA-256d [16]	C++[17]	PoW&PoS	The first cryptocurrency to use POW and POS functions.
2013	Active	Dogecoin	DOGE, XDG, Đ	Jackson Palmer & Billy Markus[18]	Script[19]	C++[20]	PoW	Based on an internet meme.
2013	Active	Emercoin	EMC	Evgenij M86 & Yitshak Dorfman	SHA-256	C++[21]	PoW&PoS	Trusted storage for any small data: acts as an alternative, decentralized DNS, PKI store, SSL infrastructure and other.
2013[22]	Active	Feather coin	FTC, □	Peter Bushnell, Brasenose College of Oxford University	NeoScript	C++[23]	N/A	Approx. 60 seconds block time
2013 [24][25]	Active	Gridcoin	GRC	Rob Hälford [26]	Script	C++[27]	Decentralized PoS	The first cryptocurrency linked to citizen science through the Berkeley Open Infrastructure for Network Computing[28][29]
2013	Active	Omni	MSC	J. R. Willett [30]	SHA-256d[31]	C++[32]	N/A	Omni is both digital currency and communications proto-col built on top of the existing bitcoin block chain.

Release	Status	Currency	Symbol	Founder(s)	Hash algorithm	Programming language of implementation blockchain	Crypto-currency (PoS, PoW, or other)	Notes
2013	Active	Primecoin	XPM	Sunny King (pseudo-nym) [15]	1CC/2CC/TWN[33]	Type-Script, C++[34]	PoW[33]	Uses the finding of prime chains composed of Cunningham chains and bi-twin chains for proof-of-work, which can lead to useful byproducts.
2013	Active	Ripple [35][36] [37]	XRP [37]	Chris Larsen & Jed McCaleb [38]	ECDSA [39]	C++[40]	"Consensus"	Designed for peer to peer debt transfer. Not based on bitcoin.
2013	Active	Nxt	NXT	BCNext (pseudonym)	SHA-256d[41]	Java[42]	PoS	Specifically designed as a flexible platform to build applications and financial services around its protocol.
2014	Active	Auroracoin	AUR	Baldur Odinson (pseudo-nym)[43]	Scrypt	C++[44]	PoW	Created as an alternative to fiat currency in Iceland.
2014	Active	Black Coin	BC	Rat4 (pseudonym)	Scrypt	C++[45]	PoS	Secures its network through a process called minting.
2014	Active	Burstcoin	BURST	Burstcoin Community	SHA-256d	Java[46]	Proof of Capacity	First Proof of Capacity coin, First Smart Contract, First Atomic Cross Chain Transfer.
2014	Inactive	Coin-ye	KOI, COYE		Scrypt		PoW	Used American hip hop artist Kanye West as its mascot, abandoned after trademark lawsuit.
2014	Active	Dash	DASH	Evan Duffield & Kyle Hagan[47]	X11	C++[48]	PoW&Proof of Service [nt 2]	A bitcoin-based currency featuring instant transactions, decentralized governance and budgeting, and private transactions.
2014	Active	NEO	NEO	Da Hongfei & Erik Zhang	SHA-256 & RIPEMD 160	C#[49]	dBFT	Chinese based cryptocurrency (formerly ANT Shares which produce ANT Coins) name change August 2017 to NEO and GAS, these enable the development of digital assets and smart contracts.
2014	Active	Maza-Coin	MZC	BTC Oyate Initiative	SHA-256d	C++[50]	PoW	The underlying software is derived from that of another cryptocurrency, ZetaCoin.
2014	Active	Monero	XMR	Monero Core Team	Crypt-to Night[51]	C++[52]	PoW	Privacy-centric coin using the CryptoNote protocol with improvements for scalability and decentralization.
2014	Active	NEM	XEM	Utopian-Future (pseudonym)	SHA3-512	Java[53]	POI	The first hybrid public/private block-chain solution built from scratch, and first to use the Proof of Importance algorithm using Eigen-Trust++ reputation system.
2015	Active	Tether	USDT	Jan Ludovicus van der Velde [54]	Omnicores [55]		PoW	Tether is backed by the USD so that one tether is exactly equal to \$1USD. It is commonly used to convert other cryptocurrencies to USD. [56]
2014	Active	Pot-Coin	POT	Pot-coin core dev team	Scrypt	C++[57]	PoS	Developed to service the legalized cannabis industry

Release	Status	Currency	Symbol	Founder(s)	Hash algorithm	Programming language of implementation blockchain	Crypto-currency (PoS, PoW, or other)	Notes
2014	Active	Syne-reo AMP	AMP	Dor Kon-forty & Greg Meredith[58]	PoS	Scala, Java[59]	PoS	Trying to create a world computer, Synereo's 2.0 tech stack incorporates all faculties needed to support decentralized computation without central servers.[60]
2014	Active	Tit-coin	TIT	Edward Mansfield & Richard Allen[61]	SHA-256d	Type-Script, C++[62]	PoW	The first cryptocurrency to be nominated for a major adult industry award.[63]
2014	Active	Verge	XVG	Sunerok	Scrypt, x17, groestl, blake2s, and lyra2rev2	C, C++[64]	PoW	
2014	Active	Stellar	XLM	Jed McCaleb	Stellar Consensus Protocol (SCP) [65]	C, C++[66]	Stellar Consensus Protocol (SCP) [65]	Open-source, decentralized global financial network. The usage is for remittances, micro-payments, services for the underbanked, mobile money/branches and professional setups.
2014	Active	Vertcoin	VTC	Bus-hido	Ly-ra2RE [67]	C++[68]	PoW	Next-gen ASIC resistance and first to implement stealth addresses.
2015	Active	Ether or "Ethereum"	ETH	Vitalik Buterin[69]	Ethash[70]	C++, Go[71]	PoW	Supports Turing-complete smart contracts.
2015	Active	Ethereum Classic	ETC		Ethash[70]		PoW	An alternative version of Ethereum[72] whose block-chain does not include the DAO Hard-fork.[73][74] Supports Turing-complete smart contracts.
2015	Active	IOTA	IOT, MIOTA [75]	David Sønstebø, Sergey Ivancheglo, Dominik Schiener and Dr. Serguei Popov	SHA-3	Java[76]	Directed acyclic graph	The first crypto-currency using the Tangle, a next generation block-chain, as distributed ledger technology.
2016	Active	Decred	DCR		Blake-256	Go[77]	PoW/PoS Hybrid	Built in governance and hybrid PoW/PoS.
2016	Active	Waves Platform	WAVES	Sasha Ivanov	PoS	Scala, Java-Script[78]	PoS	Open block-chain platform, featuring token creation, distributed exchange and fast, high volume, transactions designed for ease of use[79] and mass adoption.
2016	Active	Lisk	LSK	Max Kor-dek	DPoS	Java-Script[80]	DPoS	Lisk is a dapp creation platform in JavaScript. Lisk uses a Delegated-Proof-of-Stake (DPoS) consensus mechanism.
2016	Active	Zcash	ZEC	Zooko Wilcox	Equi-hash	C++[81]	PoW	The first open, permissionless financial system employing zero-knowledge security.

Release	Status	Currency	Symbol	Founder(s)	Hash algorithm	Programming language of implementation blockchain	Crypto-currency (PoS, PoW, or other)	Notes
2016	Active	Zclassic	ZCL	Rhett Creighton	Equihash		PoW	A fork of Zcash with no pre-mine/founder's reward.
2017	In-active	BitCon-nect	BCC					
2017	Active	Komodo	KMD			C[82]	dPoW	Uses delayed proof of work (dPoW) block-chain security.[83]
2017	Active	Bitcoin Cash	BCH[84]		SHA-256d		PoW	Hard fork from Bitcoin, Increased Block size from 1mb to 8mb
2017	Active	Ubiq	UBQ	Julian Yap [85]	Ethash [70]	Go[86]	PoW	Supports Turing-complete smart contracts; air-gapped fork of Ethereum
2017	Active	EOS.IO	EOS	Dan Larimer		WebAssembly, Rust, C, C++ [87]	delegated Proof-of-stake	Feeless Smart contract platform for decentralized applications and decentralized autonomous corporations with a block time of 500 ms.[88][87]
2017	Active	Sirin Labs	SRN			Java-Script[89]		
2017	Active	TRON	TRX	Justin Sun	SHA-256	Java[90]		
2018	Active	Cardano	ADA	Charles Hoskinson & Jeremy Wood		Has-kell[91]		
2018	Inactive	Kodak Coin	Kodak and WENN Digital	Ethash[92]				Kodak-Coin is a "photographer-centric" block-chain cryptocurrency used for payments for licensing photographs.
2018	Active	Petro		Venezuela Government	onix-Coin[93]	C++[94]		First cryptocurrency backed by Venezuela's reserves of oil.
2018	Proposed	Petro gold		Venezuela Government				Announced by President Nicolás



Cryptocurrency market capitalizations as of 27 January 2018, in billions of US dollars

What is the future of Cryptocurrency?

The market of cryptocurrencies is fast and wild. Nearly every day new cryptocurrencies emerge, old die, early adopters get wealthy and investors lose money. Every cryptocurrency comes with a promise, mostly a big story to turn the world around. Few survive the first months, and most are pumped and dumped by speculators and live on as zombie coins until the last bagholder loses hope ever to see a return on his investment.

Markets are dirty. But this doesn't change the fact that cryptocurrencies are here to stay – and here to change the world. This is already happening. People all over the world buy Bitcoin to protect themselves against the devaluation of their national currency. Mostly in Asia, a vivid market for Bitcoin remittance has emerged, and the Bitcoin using darknets of cybercrime are flourishing. More and more companies discover the power of Smart Contracts or token on Ethereum, the first real-world application of blockchain technologies emerge.

The revolution is already happening. Institutional investors start to buy cryptocurrencies. Banks and governments realize that this invention has the potential to draw their control away. Cryptocurrencies change the world. Step by step. You can either stand beside and observe – or you can become part of history in the making.

“In 2 years from now, I believe cryptocurrencies will be gaining legitimacy as a protocol for business transactions, micropayments, and overtaking Western Union as the preferred remittance tool. Regarding business transactions – you'll see two paths: There will be financial businesses which use it for it's no fee, nearly-instant ability to move any amount of money around, and there will be those that utilize it for its blockchain technology. Blockchain technology provides the largest benefit with trustless auditing, single source of truth, smart contracts, and color coins.”

– Cody Littlewood,
founder and CEO of Codelitt

Prophets Of Boom: Meet Crypto's Richest

Reported by Pamela Ambler, Angel Au-Yeung, Grace Chung, Jeff Kauflin, Alex Konrad, Laura Shin and Nathan Vardi.



In the world of cryptocurrency, fortunes can be made overnight, and the winners of this digital lottery differ from those in previous manias. The shadowy beginnings, at once anarchistic, utopian and libertarian, have drawn an odd lot of pioneers—from antiestablishment cypherpunks and electricity-guzzling “miners” to prescient Silicon Valley financiers and a larger-than-usual assortment of the just plain lucky “hodlers,” the typo-inspired crypto jargon for “buy-and-hold” investors.

Based on numbers on estimated holdings of cryptocurrencies (a few provided proof), post-tax profits from trading crypto-assets and stakes in crypto-related businesses, and locked in the estimates using prices on Jan. 19, 2018.

It's a near certainty that we've missed some people and that some of our estimates are wide of the mark. Shining a light on the invisible rich, we believe that fortunes of this magnitude should never be allowed to lurk in the shadows. ■



SPEAK UP ABOUT FAKE MEDICINES

VISIT FIGHTTHEFAKES.ORG

FAKE MEDICINES HARM – NOT HEAL

There are a lot of shady ingredients found in fake medicines that are directly responsible for serious disability and even death. This includes poisons such as mercury, rat poison, paint and antifreeze.



MERCURY



RAT POISONING



PAINT



ANTIFREEZE



Fake tuberculosis and malaria drugs
alone are estimated to

KILL 700,000 PEOPLE A YEAR*.



*International Policy Network

Cryptocurrencies as a Disruptive Innovation

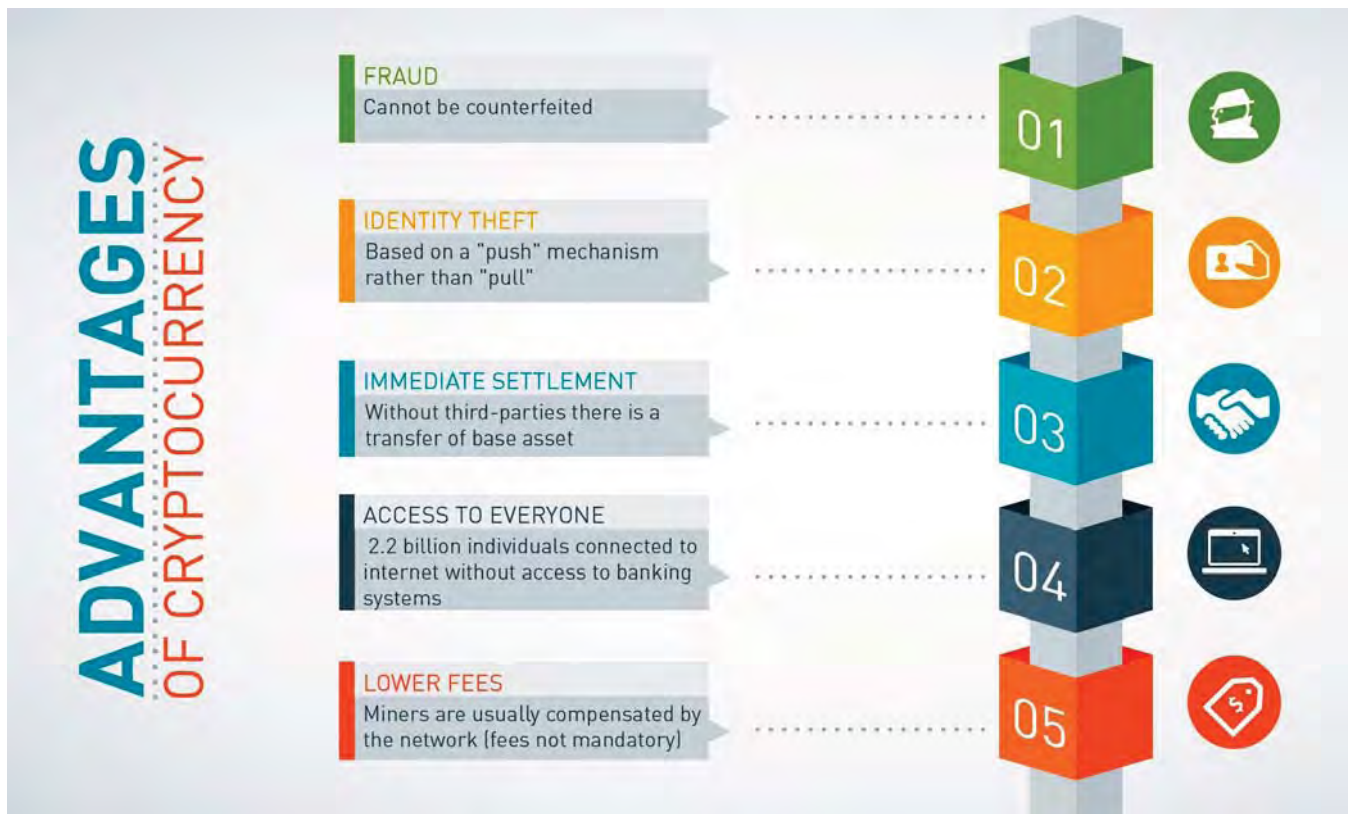
PROFESSOR CLAYTON CHRISTENSEN had coined and defined the term Disruptive Innovation as a “process by which a product or service takes root initially in simple applications at the bottom of a market and then relentlessly moves up market, eventually displacing established competitors.” There have been numerous instances where disruptive technologies have displaced well-

established competitors, WhatsApp displacing Short Messaging Service (SMS) being one such example. Disruptive technologies offer value to the users, in terms of cost-effectiveness, usability and simplicity. Considering cryptocurrencies in this perspective, they may well have the potential to displace the existing financial systems which enable electronic flow of money across different political boundaries.

ADVANTAGES of Cryptocurrencies

The success of cryptocurrencies could be attributed to the advantages they have, such as:

1. **Privacy Protection:** Privacy and anonymity of the transacting parties was the prime concern of the proponents of cryptocurrencies when the idea was promulgated, and these became part of the



underlying principles. The use of pseudonyms conceals the identities, information and details of the parties to the transaction – perquisites for privacy enthusiasts.

2. **Cost-effectiveness:** Electronic transactions attract fees and charges, which is on the higher side when the transactions are transnational and undergo currency conversion, or attract processing fee levied by the banks, third party clearing houses or gateways. Debit or credit card transactions also attract a processing or transaction fee when used overseas, which is somewhere of the order of 1% to 3%, while electronic transfers could exceed to 10% or 15%. Cryptocurrencies solve this problem, as they have single valuation globally, and the transaction fee is extremely low, being as low as 1% of the transaction amount.

Cryptocurrencies eliminate third party clearing houses or gateways, cutting down the costs and time delay. All the transactions over cryptocurrency platforms, whether domestic or international, are equal. Another facet, which brings the cost down considerably low, is inbuilt security and fraud prevention mechanism, which accounts for 40% of the costs of payment processing gateways.

3. **Lower Entry Barriers:** Possessing a bank account or a debit/credit card for international usage requires documented proofs for income, address or identification. Banks or financial institutions might have their own set of eligibility criteria for these facilities. Cryptocurrencies lower these entry barriers, they are free to join, high on usability and the users do not require any disclosure or proof for income, address or identity.
4. **Alternative to Banking Systems and Fiat Currencies:** Governments have a tight control and regulation over banking systems, international money transfers and their national currencies or monetary policies.

Cryptocurrencies offer the user a reliable and secure means of exchange of money outside the direct control of national or private banking systems.

5. **Open Source Methodology and Public Participation:** A majority of the cryptocurrencies are based on open source methodology, their software source code is publicly available for review, further development, enhancement and scrutiny. The ecosystem of cryptocurrencies is primarily participation based, as software development, bug reporting and fixing, testing etc. are driven by the wider user base, rather than a closed set of individuals or an institution. They have their own consensus based decision making, built-in quality control and self-policing mechanisms for building frameworks, practices, protocols and processes.
6. **Immunity to Government led Financial Retribution:** Governments have the authority and means to freeze or seize a bank account, but it is infeasible to do so in the case of cryptocurrencies. For citizens in repressive countries, where governments can easily freeze or seize the bank accounts, cryptocurrencies are immune to any such seizure by the state.

Despite these numerous advantages and user friendly processes, cryptocurrencies have their own set of associated risks in the form of volatility in valuation, lack of liquidity, security and many more. Cryptocurrencies are being denounced in many countries because of their use in grey and black markets. There are two sets of interconnected risks; one being to the growth and expansion of these platforms in the uncertain policy environment, and the other being the risks these platforms pose to the users and the security of the state.

Risks involved in Cryptocurrencies

1. **Key/Wallet/Exchange Security:** A virtual wallet stores the keys and transaction records of the user. The

secure digital keys are used to access the public address and to sign or authenticate the transactions initiated by the user. Virtual wallets exist in the forms of desktop wallets (a software), Web-based wallets (a website/cloud) and mobile wallets (an app). Cold storage of cryptocurrencies is claimed to be more secure, which is in the form of storage media, USB drive, on the paper or hardware wallets, with some of them even using biometrics for authentication. Specialised online exchanges facilitate the purchase or sale of cryptocurrencies. In the entire chain of security, wallets and exchanges are found to be the weakest link, and that is where the attacks are commonly aimed at. In 2014, hackers stole about 480 million USD in Bitcoins from Tokyo's Mt. Gox exchange; which, at that time, was one of the biggest Bitcoin exchange in the world.

There have been many more such incidents in recent times; attackers moved about 60 million USD worth of the virtual currency Ether from the account of Decentralized Autonomous Organization (DAO) in June 2016; a breach at Bithumb, South Korea's largest Bitcoin and Ethereum exchange, led to a loss of around 1 million USD worth of cryptocurrencies in June 2017; and hackers hijacked cryptocurrency trading platform CoinDash in the middle of its initial coin offering and stole 7 million USD from CoinDash on 17 July, 2017. In general, the reported instances of thefts have been from the exchanges or the users' end. Users are prone to the risk of losing their holdings if they lose the private encryption key or forget it or lose the storage device/hardware where the wallet is kept or even lose the key due to a theft or hack.

2. **Hijacking/Routing Attacks/ Distributed Denial of Service (DDoS) attacks on Cryptocurrency System:**

Cryptocurrency systems are open source and the pooled in resources of the miners keeps these systems up and running. Some of the

research efforts in the recent past have delivered proofs-of-concept for hijacking or Internet routing attacks to which cryptocurrency systems are vulnerable to. Additionally, cryptocurrency platforms have also been found to be prone to DDoS attacks, targeted at the exchanges might slow down services or render the platform completely inaccessible. Bitfinex, a Bitcoin exchange, faced DDoS attacks in February 2017; Indian exchange Coinsecure had faced similar attacks in 2016, and BTC-E, Krazen, Poloneix have been a victim of DDoS attacks. Owing to these threats, cryptocurrency founders/firms have rolled out a Cryptocurrency Security Standard, a set of requirements for all information systems that make use of cryptocurrencies, including exchanges, web applications, and cryptocurrency storage solutions, complementing existing information security standards such as ISO 27001:2013.

3. Uncertain Regulatory

Environment: The future and further success of cryptocurrencies depends upon the way regulatory frameworks are devised. Different countries have approached this innovation in different ways, and therefore the regulatory environment remains uncertain.

4. Lack of Liquidity and Lower Acceptability:

Cryptocurrencies function outside banking systems, beyond the regulations or controls of the regulatory agencies. Although online exchanges facilitate exchange of cryptocurrencies with fiat currencies, but generally, this is restricted to the more popular cryptocurrencies only, basically, the ones with high market capitalisation. For the rest of cryptocurrencies, and for all of them in certain countries, there is an absolute lack of liquidity. Moreover, the acceptance of cryptocurrencies at merchant sites is also restricted. As

cryptocurrencies are gaining popularity and entering into niche markets, exchanges have sprung up dealing in national currencies such as Rupee, Yuan and Yen, adding much required liquidity to the cryptocurrencies, but still restricted to the popular ones.

5. Price Volatility:

Volatility, a measure of variance of the price of a financial instrument over a certain period of time, is associated with the risk level of the instrument. High volatility is

in illicit trade. Cryptocurrencies do not yet have an accepted vulnerability index, which other financial instruments such as fiat currencies and gold have. Experts believe and argue that, when the consumer base of these instruments widens, the market and prices of cryptocurrencies will automatically stabilise.

6. Uncertainty over Consumer Protection and Dispute Settlement Mechanisms:

Cryptocurrencies are decentralised,



regarded as risky, and cryptocurrencies are known to be extremely prone to price fluctuations. The prices of Bitcoin touched an all-time high of 2,700 USD in May 2017, followed by a sharp correction, shedding around 30% of its value in the next two days. There have been four of such rallies for Bitcoin, while others such as Ethereum, Litecoin, Dash, Ripple and Monero etc. have had their own price fluctuations. These fluctuations are driven by many factors, varying from geopolitical events to the policies or regulations of governments, from security breaches at exchanges to the vulnerabilities found in the code, or their reported use/abuse

that means, there is no single authority for mediation or dispute redressal. The miners are not responsible for any arbitration of disputes between the parties. The transactions are also irreversible, which, in the case of banks or payment gateways is reversible if the dispute is resolved, safeguarding the users from fraud. Cryptocurrencies lack these safeguards, exposing the users to the risks of fraud and bringing a sense of uncertainty over consumer protection and dispute settlement mechanisms.

Perhaps, unless and until these risks are mitigated, the future of cryptocurrencies as legal instruments for exchange of goods and services or for

that matter, payments, will continue to remain uncertain. Some of these are technical challenges, such as dispute settlement and security of platforms, while others are policy issues which are much more difficult to resolve such as regulation, liquidity, price volatility and consumer protection. Moreover, cryptocurrencies are an entirely new payment method, with privacy benefits for users, but at the same time, this poses significant risks to security practices, counter-terrorism, law enforcement and taxation.

Risks from Cryptocurrencies

1. Potential use for Illicit Trade and Criminal Activities:

The perpetrators of Wannacry ransomware - which created havoc across 150 countries in May 2017 - demanded ransom of 300-600 USD through Bitcoins.

Cryptocurrencies are virtual and decentralised, well beyond the control or authority of the state. Probably, this has made their absorption quicker into grey and black markets, ransomwares and a host of other

illicit activities of crime and money laundering. The infamous marketplace "Silk Road" over DarkWeb relied heavily on Bitcoins for payments in exchange of illicit trade of narcotics, hacking tools, small arms, child pornography, stolen credit cards information and so forth. Between 2011 and 2013, the value of Bitcoins surged as criminals were purchasing Bitcoins in large volumes. In late 2015 and early 2016, Dutch police unearthed two small groups that indulged in Bitcoin-related money laundering. Regulatory bodies and law enforcement agencies have raised legitimate concerns that cryptocurrency accounts and wallets cannot be

frozen, seized or examined.

2. Potential use for Terror Financing:

In the aftermath of the attack on World Trade Centre on September 11, 2001, rigorous vigilance and regulatory controls were imposed on global financial systems to crack down on terror financing. This moved terror outfits towards money laundering and hawala networks, but owing to the similar reasons as stated above, cryptocurrencies are also emerging as a new funding stream for terrorist outfits. In a blogpost, titled "Bitcoin and the Charity of Violent Physical Struggle", Islamic State of Iraq and Syria (ISIS) had proposed using Bitcoins to raise funds., Known instances of terror outfits using these modalities are very limited, with one such instance

enforcement apparatus are inadequately prepared to tackle.

3. Potential for Tax Evasion:

Cryptocurrencies are not regulated or controlled by governments, making them a lucrative option for tax evasion. Sales made or salaries paid in the form of cryptocurrencies could be used to avoid income tax liability. Taxation rules and regulations may vary from state to state, and many countries do not yet have policies in place for cryptocurrencies. There is, as yet, no agreement or understanding on whether the income earned through trading, or for that matter, even mining of cryptocurrencies, should be included in gross income or treated as capital gains. Some proponents of cryptocurrencies have gone to the extent of raising doubts

over the authority of the state to enforce taxation on something they do not issue or have control on. Owing to the concerns regarding the perceived potential of cryptocurrencies for tax evasion, the Internal Revenue Service of the US Government had issued a notice in 2014, labelling them



emerging out of Indonesia recently. The proponents and entrepreneurs of cryptocurrencies, however, denounce the proposals of ban and control on cryptocurrencies, as they argue that many technologies such as smartphones are also being used by terrorists and criminals, and they are not liable to be banned just because malicious actors use them. Arguments and counter-arguments might vary, and analyses of the alleged use of cryptocurrencies in criminal activities and terror financing might lead to divergent conclusions, but certainly, cryptocurrencies have thrown open a whole new challenge towards which majority of the intelligence and law

as "intangible property"; and deemed trading in cryptocurrencies to be taxable; and also clarified that digital currencies are capital assets and are therefore subject to capital gains taxes. A similar debate over the categorisation of cryptocurrencies as security, currency or a commodity derivative is currently playing out in India. Cryptocurrencies do not have legal tender status in any jurisdiction, but many jurisdictions have already declared the transactions for the sale of goods or services, capital gains, income etc. as taxable. As taxation authorities are grappling with devising strategies and guidelines for tax compliance, tax evaders might find their tax havens in form of cryptocurrencies. ▶



For Cryptocurrencies In India?

Government Regulations and Cryptocurrencies in India

For long clarity was sought on the status of cryptocurrencies in India, which now hopefully the Finance Minister has provided.

But in the meantime Bitcoin and other cryptocurrencies have grown to be a phenomenon in India. One can imagine the scale of usage of virtual currencies in India merely by the fact that one in every ten Bitcoin transactions that happen throughout the world takes place in India. Government's stance on Bitcoin and other virtual currencies was rather known. The Government in the past has indicated that it remained paranoid about the usage of cryptocurrencies is money laundering, tax evasion and financing of illegitimate activities such as terrorism and more. Recently the IT department had also send notices to 4-5 Lakh HNIs who have indulged in Bitcoin or other cryptocurrency trading. Reports have also emerged about banks freezing accounts of cryptocurrency exchanges and the registrar of companies (ROC) stopping registration of companies which intended to operate in the said domain.



Future of Bitcoin usage and trading in India

It is believed that in the last 17 months \$3.5 billion worth of transactions in virtual currencies has taken place in India. After the finance minister's announcement experts believe that a

clampdown on usage of Bitcoins and other cryptocurrencies as a payment method is in the offering. Investors who were looking for some kind of legitimization for cryptocurrencies in India will be disappointed with the Budget. In his Budget speech Finance Minister Arun Jaitley stated that the Government of India doesn't recognise cryptocurrencies as legal tenders. He further stated that the Government will take all measures necessary to stop usage of these virtual currencies in financing illegitimate activities or as part of the payments system. Few weeks before the Budget, the Finance Minister had advised people against the usage and investing in cryptocurrencies after equating them with Ponzi schemes. Although no specific ban on Bitcoin or any other cryptocurrency was mentioned in the Budget speech but what is likely to cause concern amongst cryptocurrency users and investors in the fact that the FM categorically mentioned that the government will take steps to eliminate the usage of the same.

In A Bold Move, RBI Bans Cryptocurrencies; Mixed Reactions Follow

While some welcomed the RBI's move, others stressed on the need for more regulation rather than a ban.



IN WHAT IS being described a knee jerk reaction by many, the Reserve Bank of India or RBI has said it will stop the trade of cryptocurrencies by the institutions governed by it. The RBI has given banks a time-frame

of three months to implement the decision and said it was taking the step to ring-fence banks.

"RBI regulated institutions are required to stop having business relations with the entities dealing in virtual currencies forthwith and unwind the existing relation in three months," RBI Deputy Governor B P Kanungo said.

While some welcomed the RBI's move, others stressed on the need for more regulation rather than a ban.

"You have countries in Europe that have regulated cryptocurrency and these regulations ensure there is no money laundering and not Ponzi schemes. What you need to do is regulate and not ban," senior lawyer in the Bombay High Court, Sujay Kantawala said.

Mukul Shrivastava, Partner, Fraud Investigation & Dispute Services at Ernst & Young said, "The last couple of months has seen Investments in cryptocurrency more as a 'herd mentality' - it was almost a bubble waiting to burst."

However, the RBI has kept a window open for digital currencies in the country.

In its statement on developmental and regulatory policies, the Reserve Bank of India said, "Rapid changes in the

landscape of the payments industry along with factors such as the emergence of private digital tokens and the rising costs of managing fiat/paper/metallic money have led central banks around the world to explore the option of introducing fiat digital currencies."

"While many central banks are still engaged in the debate, an inter-departmental group has been constituted by the RBI to study and provide guidance on the desirability and feasibility to introduce a central bank digital currency. The report will be submitted by end June," it added.

Some people who have invested in cryptocurrencies are disappointed with the bank's step to ban cryptocurrencies altogether.

In another important move, the RBI has also made it mandatory for payment system operators to store data within the country. ▶

THE AWARE CONSUMER

An opportunity to **SPEAKUP!**

Join the Movement ...

Save upto

50%

on subscription



Subscribe **today!**

{ Save **₹ 3,600/-**
FOR 36 ISSUES }

India's more credible consumer monthly from renowned Consumer Activist Bejon Kumar Misra

Please accept my subscription of **THE AWARE CONSUMER**

NAME _____

ADDRESS _____

PH. NO. _____ E-MAIL _____

PAYMENT ☐ CASH ☐ CHEQUE CHEQUE/DD NO. _____

DRAWN ON _____

DATE _____ SIGNATURE _____

No. of Issues	News Stand Price	Discount	You Pay	You Save
12	₹ 2,400/-	20%	₹ 1,920/-	₹ 480/-
24	₹ 4,800/-	30%	₹ 3,360/-	₹ 1,440/-
36	₹ 7,200/-	50%	₹ 3,600/-	₹ 3,600/-

Cheque / DDs should be drawn in favour of **BEJON KUMAR MISRA**

Send your subscription to: The AWARE CONSUMER, F-9, 2nd Floor, Kailash Colony, New Delhi-110048

Contact: 9811044424 • +91-11-40537140 • E-mail: bejonmisra@gmail.com



Department of Pharmaceuticals
Ministry of Chemicals & Fertilizers
Government of India

DAWN OF A NEW ERA OF GOOD HEALTH FOR THE POOR

“The poor must have access to affordable medicines, the poor must not lose their lives because of lack of medicines... that's why Jan Aushadhi Kendras have been planned across the country”
- Narendra Modi



Quality Medicines at Affordable Prices

- Quality medicines available at Jan Aushadhi Kendra's
- Quality of medicines ensured from NABL accredited laboratories.
- Over 600 High Quality English Medicines
- 154 Surgical and Consumables Products
- At 50% or Lower Price than the Branded Products
- More than 1400 Jan Aushadhi Kendra in 28 State/UTs are functional

Jan Aushadhi Kendra's now available at your Door Steps

Salient features of the scheme:

- Ensure access to quality medicines
- Extend coverage of quality generic medicines so as to reduce and thereby redefine the unit cost of treatment per person
- Create awareness about generic medicines through education and publicity so that quality is not synonymous with only high price
- Be a public programme involving Government, PSUs, Private Sector, NGO, Societies, Co-operative Bodies and other Institutions
- Create demand for generic medicines by improving access to better healthcare through low treatment cost and easy availability wherever needed in all therapeutic categories.



COME AND CONTRIBUTE FOR BUILDING A HEALTHY AND HAPPY INDIA

For more information call 1800-180-8080/0124-4556750 (Monday to Saturday- 9:30 A.M. to 5:30 P.M.), or log in to janaushadhi.gov.in



Pyush Misra
Director
Consumer Online Foundation

BITCOIN: is it a bubble waiting to burst or a good investment?

Disciples of the
cryptocurrency plan
to hold on for
dear life but
traditional finance
is getting twitchy



BITCOIN IS THE fastest-growing asset in the world this year, but the virtual currency does not appear to have many users in London's tech district. It has been more than a month since bitcoin was used to buy a flat white or craft beer sold at the Old Shoreditch Station, according to the hospitality manager at the east London bar.

What is bitcoin and is it a bad investment?

Bitcoin is the first, and the biggest, "cryptocurrency" – a decentralised tradeable digital asset. Whether it is a bad investment is the big question.

Bitcoin can only be used as a medium of exchange and in practice has been far more important for the dark economy than it has for most legitimate uses. The lack of any central authority makes bitcoin remarkably resilient to censorship, corruption or regulation. That means it has attracted a range of backers, from libertarian monetarists who enjoy the idea of a currency with no inflation and no central bank, to drug dealers who like the fact that it is hard (but not impossible) to trace a bitcoin transaction back to a physical person.

Louis Chauvin admits he cannot find the iPad that is used by staff for

processing bitcoin payments, as he resumes serving customers queueing to pay with their contactless bank cards. Although the establishment sits in the capital's buzzing tech hub, and is 'advertised online as one of the few retailers in London accepting the hipster-cum-computer nerds currency, as few as 20 people have asked to pay with it in the two years he has worked there.

Over the same period, the value of a single bitcoin has rocketed from around \$300 to more than \$11,000 in one week. The currency was trading at \$10,700.

Chauvin says bitcoin's increasing value and media coverage has not



A bitcoin machine at a cafe near Old Street, London.
Photograph: Martin Godwin for the Guardian

escaped customers. More people have come in asking how it works, thinking of using it in their own shop, rather than actually paying with it, he says, adding: "It's cool, it attracts some people. But for now it's niche."

Bitcoin is a digital currency, also known as a cryptocurrency, that emerged after the financial crisis and is not underpinned by a central bank. It allows people to bypass banks and traditional payment methods for goods and services, an idea that has evidently caught the imagination of some investors, because its price has surged by more than 900% in 2017. Bitcoin, created by "miners" who use high-powered computers to solve complex mathematical problems, must be stored online using a digital wallet, and can be bought or sold using exchanges such as Bitstamp, Bithumb and Kraken.

But as bitcoin hits the stratosphere, there are fears an

economic bubble is forming as it becomes treated less like a currency and more like a store of value, open for speculators making ever increasing bets on how far it can rise. Central bankers, who had to step in when the subprime mortgage bubble

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part.

burst, have also warned of its dangers.

Economists have compared bitcoin's meteoric rise with past bubbles, such as the tulip mania of the 17th century and the dotcom bubble that began in the late 90s with the Nasdaq index in New York and burst in 2000. Both examples foreshadow a painful collapse for a currency that has no intrinsic value to those who hold it beyond that ascribed to it by a community of owners. Should they realise the emperor has no clothes en masse, there could be a rude awakening.

Oliver White at Fathom Financial Consulting wrote that bitcoin "certainly fits the criterion" for a bubble asset. Using data stretching back to 2013, Fathom's economists compared the price of bitcoin with its historical



average and plotted that against other mainstream assets - such as shares and bonds. They found the current value of bitcoin running at six times its average price since 2013. The cryptocurrency has yo-yoed with extreme volatility over the period, the price has leapt to as high as \$11,379 and plunged to \$9,146 before rebounding to \$10,700.

Bitcoin disciples argue its price will rise further, viewing volatility as a necessary bump on the path to even higher valuations. Fans even coined a term to describe their tactic of holding on for dear life, Hodl. A deliberate mistyped neologism, up there with noob, to mean newbie, adding to the pantheon of computer slang.

There are some rational reasons to keep calm and carrying on hodling. Serious investors are just getting interested in a market that has so far been dominated by crypto nerds and retail investors.

The libertarian dream of bitcoin's creators is of a currency existing outside the traditional world of finance. But the bigger bitcoin grows and the more conventional institutions such as the CME get involved, the more chance there is of investors losing money and for regulators to intervene.

Global financial leaders such as



"Tulip Mania". The warnings from history

JPMorgan boss Jamie Dimon and Goldman Sachs's Lloyd Blankfein have warned that the currency is ripe for use by fraudsters.

Ajit Tripathi of accountancy firm PwC says bitcoin's meteoric rise and its creation myth have attracted more buyers. The currency is said to have been created by a mysterious figure called Satoshi Nakamoto, although there is no proof this is actually a real person. The absence of any government or bank standing behind the currency also fuels its appeal to those unhappy with the financial

system after the credit crunch.

"Bubbles are driven by sentiment and stories, and bitcoin has a great story with a lot of mystery and spectacle to it," Tripathi says. "Is bitcoin at \$40,000 by the middle of next year unthinkable? It's not but is there a logical and rational explanation for why it should be, I don't think so."

Back in east London at the Old Street roundabout, known as "Silicon Roundabout" for its proximity to so many tech startups, Ben Page-Phillips says he fears a collapse in bitcoin's value. He also accepts the currency at the independent cafe he runs with his brother, Nincomsoup, which they first opened together just before the dotcom crash 18 years ago.

The restaurant is not exposed to a bitcoin bubble because customers pay via an app that takes on the risk by instantly converting bitcoin payments into pounds on behalf of the shop. But he likes the lower cost it brings to processing sales, unlike the "crazy fees" charged by credit card companies.

"I love that it's outside the banking system, but I have concerns," he says. "You see everyone piling in and the concern is that it's going to be artificially inflated."

I would treat it like a game – it's shot up so much, and what goes up must come down." ▸



Bitcoin machine at a cafe near Old Street roundabout.
Photograph: Martin Godwin for the Guardian

How cryptocurrencies emerged as a side product of digital cash



FEW PEOPLE KNOW, but cryptocurrencies emerged as a side product of another invention. Satoshi Nakamoto, the unknown inventor of Bitcoin, the first and still most important cryptocurrency, never intended to invent a currency.

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

His goal was to invent something; many people failed to create before digital cash.

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

— Satoshi Nakamoto, 09 January 2009, announcing Bitcoin on SourceForge.

The single most important part of Satoshi's invention was that he found a way to build a decentralized digital

cash system. In the nineties, there have been many attempts to create digital money, but they all failed.

... after more than a decade of failed Trusted Third Party based systems (Digicash, etc), they see it as a lost cause. I hope they can make the distinction, that this is the first time I know of that we're trying a non-trust based system.

— Satoshi Nakamoto in an E-Mail to Dustin Trammell

After seeing all the centralized attempts fail, Satoshi tried to build a digital cash system without a central entity. Like a Peer-to-Peer network for file sharing.

This decision became the birth of cryptocurrency. They are the missing piece Satoshi found to realize digital cash. The reason why is a bit technical and complex, but if you get it, you'll know more about cryptocurrencies than most people do. So, let's try to make it as easy as possible:

To realize digital cash you need a payment network

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

In a decentralized network, you don't have this server. So you need every single entity of the network to do this job. Every peer in the network needs to have a list with all transactions to check if future transactions are valid or an attempt to double spend.

But how can these entities keep a consensus about this records?

If the peers of the network disagree about only one single, minor balance, everything is broken. They need an absolute consensus. Usually, you take, again, a central authority to declare the correct state of balances. But how can you achieve consensus without a central authority?

Nobody did know until Satoshi emerged out of nowhere. In fact, nobody believed it was even possible.

Satoshi proved it was. His major innovation was to achieve consensus without a central authority. Cryptocurrencies are a part of this solution – the part that made the solution thrilling, fascinating and helped it to roll over the world.

What are cryptocurrencies really?

If you take away all the noise around cryptocurrencies and reduce it to a simple definition, you find it to be just limited entries in a database no one can change without fulfilling specific conditions. This may seem ordinary, but, believe it or not: this is exactly how you can define a currency.

Take the money on your bank account: What is it more than entries in a database that can only be changed under specific conditions? You can even take physical coins and notes: What are they else than limited entries in a public physical database that can only be changed if you match the condition than you physically own the coins and notes? Money is all about a verified entry in some kind of database of accounts, balances, and transactions.

How miners create coins and confirm transactions

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

A transaction is a file that says, "Bob gives X Bitcoin to Alice" and is signed by Bob's private key. It's basic public key cryptography, nothing special at all. After signed, a transaction is broadcasted in the network, sent from one peer to every other peer. This is basic p2p-technology. Nothing special at all, again.

The transaction is known almost immediately by the whole network. But only after a specific amount of time it gets confirmed.

Confirmation is a critical concept in cryptocurrencies. You could say that cryptocurrencies are all about confirmation.

As long as a transaction is unconfirmed, it is pending and can be forged. When a transaction is confirmed, it is set in stone. It is no longer forgeable, it can't be reversed, it is part of an immutable record of historical transactions: of the so-called blockchain.

Only miners can confirm transactions. This is their job in a cryptocurrency-network. They take transactions, stamp them as legit and spread them in the network. After a transaction is confirmed by a miner, every node has to add it to its database. It has become part of the blockchain.

For this job, the miners get rewarded with a token of the cryptocurrency, for example with Bitcoins. Since the miner's activity is the single most important part of cryptocurrency-system we should stay for a moment and take a deeper look on it.

What are miners doing?

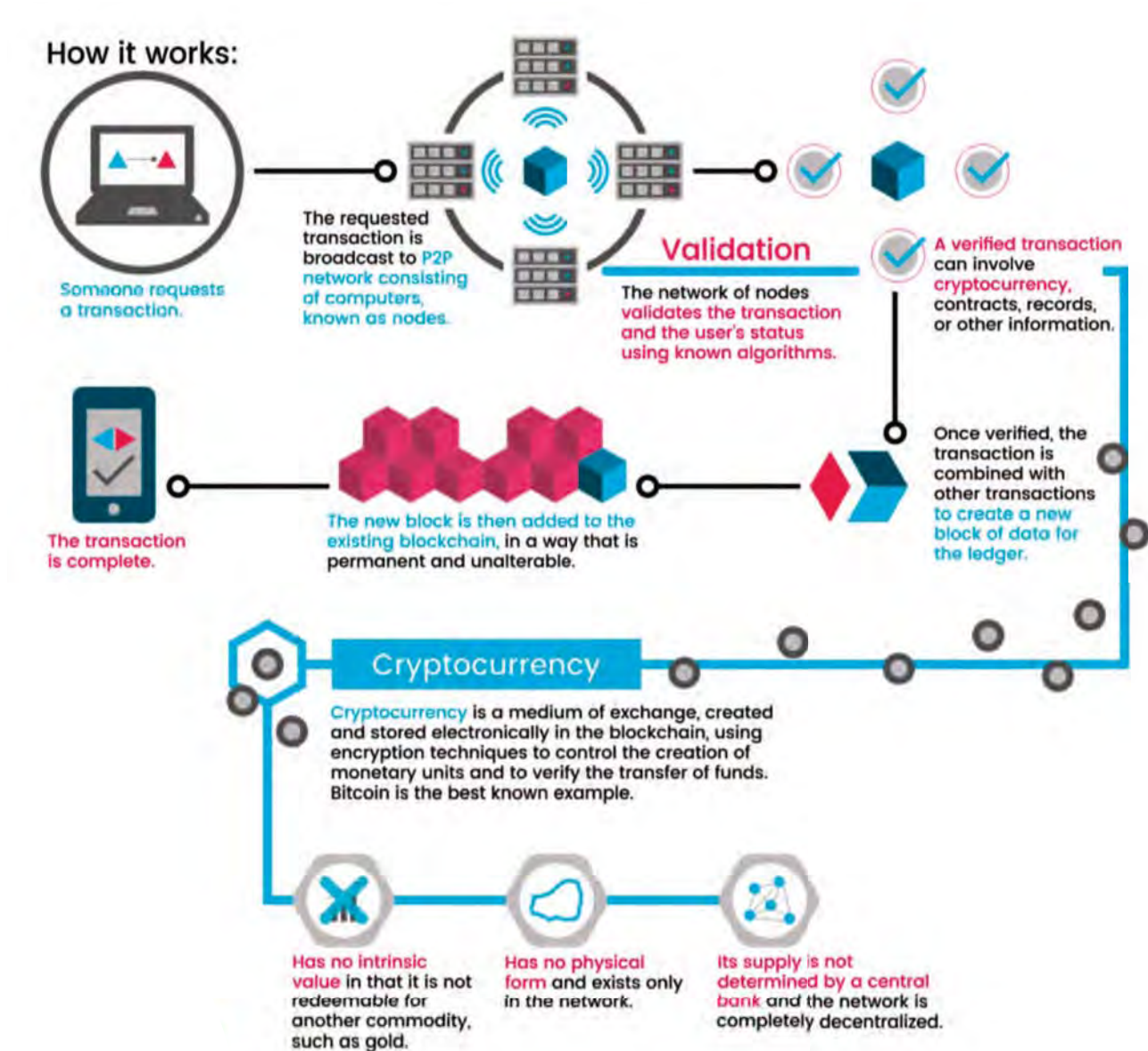
Principally everybody can be a miner. Since a decentralized network has no authority to delegate this task, a cryptocurrency needs some kind of mechanism to prevent one ruling party from abusing it. Imagine someone creates thousands of peers and spreads forged transactions. The system would break immediately.

So, Satoshi set the rule that the miners need to invest some work of their computers to qualify for this task. In fact, they have to find a hash – a product of a cryptographic function – that connects the new block with its predecessor. This is called the Proof-of-Work. In Bitcoin, it is based on the SHA 256 Hash algorithm.

You don't need to understand details about SHA 256. It's only important you know that it can be the basis of a cryptologic puzzle the miners compete to solve. After finding a solution, a miner can build a block and add it to the blockchain. As an incentive, he has the right to add a so-called coinbase transaction that gives him a specific number of Bitcoins. This is the only way to create valid Bitcoins.

Bitcoins can only be created if miners solve a cryptographic puzzle. Since the difficulty of this puzzle





increases the amount of computer power the whole miner's invest, there is only a specific amount of cryptocurrency token that can be created in a given amount of time. This is part of the consensus no peer in the network can break.

Revolutionary properties

If you really think about it, Bitcoin, as a decentralized network of peers which keep a consensus about accounts and balances, is more a currency than the numbers you see in your bank account. What are these numbers more than entries in a database – a database which can be changed by people you don't see and by rules you don't know?

Basically, cryptocurrencies are entries about token in decentralized consensus-databases. They are called CRYPTOcurrencies because the consensus-keeping

process is secured by strong cryptography.

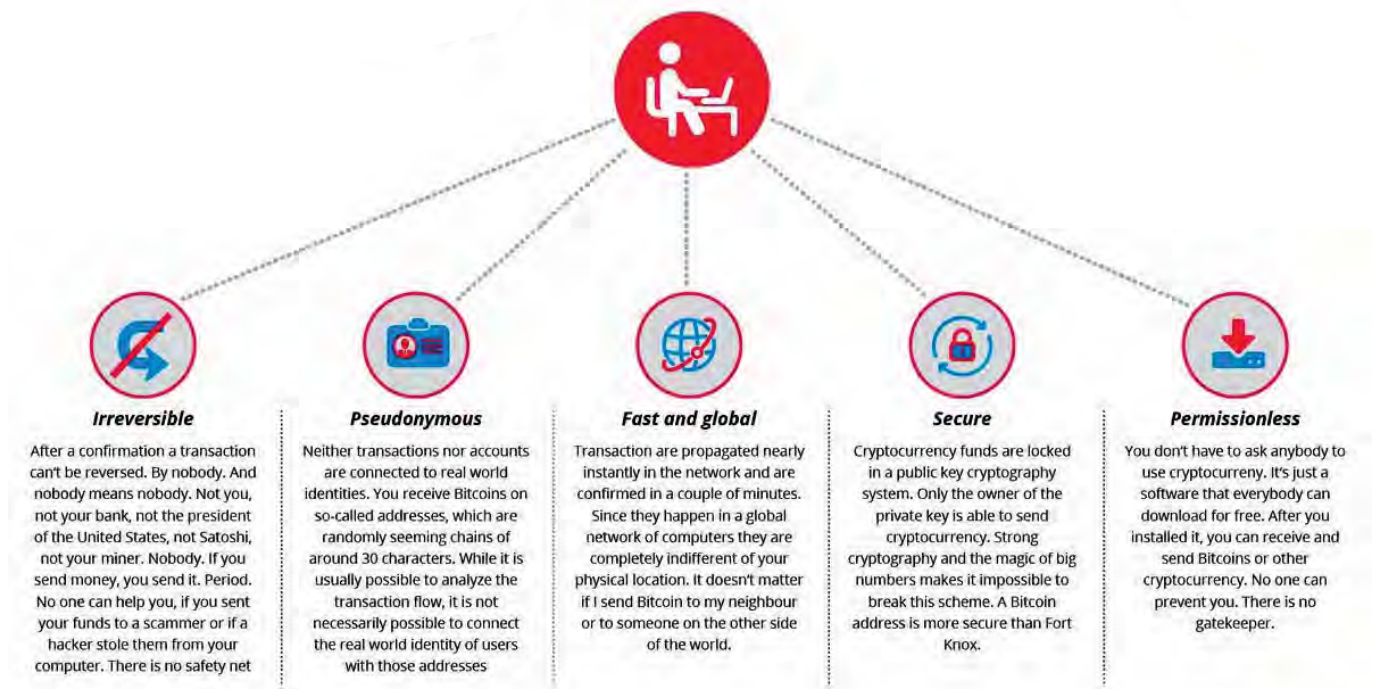
Cryptocurrencies are built on cryptography. They are not secured by people or by trust, but by math. It is more probable that an asteroid falls on your house than that a bitcoin address is compromised.

Describing the properties of cryptocurrencies we need to separate between transactional and monetary properties. While most cryptocurrencies share a common set of properties, they are not carved in stone.

Transactional properties:

1. Irreversible: After confirmation, a transaction can't be reversed. By nobody. And nobody means nobody. Not you, not your bank, not the president of the United States, not Satoshi, not your miner. Nobody. If you send money, you send it. Period. No one can help you, if you sent your funds to a scammer or if a

Cryptocurrency opens the door for revolutionary technological possibilities



hacker stole them from your computer. There is no safety net.

2. Pseudonymous: Neither transactions nor accounts are connected to real-world identities. You receive Bitcoins on so-called addresses, which are randomly seeming chains of around 30 characters. While it is usually possible to analyze the transaction flow, it is not necessarily possible to connect the real world identity of users with those addresses.
3. Fast and global: Transaction are propagated nearly instantly in the network and are confirmed in a couple of minutes. Since they happen in a global network of computers they are completely indifferent of your physical location. It doesn't matter if I send Bitcoin to my neighbour or to someone on the other side of the world.
4. Secure: Cryptocurrency funds are locked in a public key cryptography system. Only the owner of the private key can send cryptocurrency. Strong cryptography and the magic of big numbers makes it impossible to break this scheme. A Bitcoin address is more secure than Fort Knox.
5. Permissionless: You don't have to ask anybody to use cryptocurrency. It's just a software that everybody can download for free. After you installed it, you can receive and send Bitcoins or other cryptocurrencies. No one can prevent you. There is no gatekeeper.

Monetary properties:

1. Controlled supply: Most cryptocurrencies limit the supply of the tokens. In Bitcoin, the supply decreases in time and will reach its final number somewhere in around 2140. All cryptocurrencies control the supply of the token by a schedule written in the code. This means the monetary supply of a cryptocurrency in every given moment in the future can roughly be calculated today. There is no surprise.
2. No debt but bearer: The Fiat-money on your bank account is created by debt, and the numbers, you see on your ledger represent nothing but debts. It's a system of IOU. Cryptocurrencies don't represent debts. They just represent themselves. They are money as hard as coins of gold.

To understand the revolutionary impact of cryptocurrencies you need to consider both properties. Bitcoin as a permissionless, irreversible and pseudonymous means of payment is an attack on the control of banks and governments over the monetary transactions of their citizens. You can't hinder someone to use Bitcoin, you can't prohibit someone to accept a payment, you can't undo a transaction.

As money with a limited, controlled supply that is not changeable by a government, a bank or any other central institution, cryptocurrencies attack the scope of the monetary policy. They take away the control central banks take on inflation or deflation by manipulating the monetary supply. ▶

What The Central Banks Are Saying About Cryptocurrencies

Eight years since the birth of bitcoin, central banks around the world are increasingly recognizing the potential upsides and downsides of digital currencies.



THE GUARDIANS OF the global economy have two sets of issues to address. First is what to do, if anything, about emergence and growth of the private cryptocurrencies that are grabbing more and more attention with bitcoin now surging toward \$10,000. The second question is whether to issue official versions.

Following is an overview of how the world's largest central banks (and some smaller ones) are approaching the subject:



The Reserve Bank of India (RBI) is opposed to cryptocurrencies given that they can be a channel for money laundering and terrorist financing. Photo: AFP

US: privacy worry

The Federal Reserve's investigation into cryptocurrencies is in its early days, and it hasn't been overtly enthusiastic about the idea of a central-bank issued answer to bitcoin. Jerome Powell,

a board member and the chairman nominee, said earlier this year that technical issues remain with the technology and "governance and risk management will be critical." Powell said there are "meaningful" challenges to a central bank cryptocurrency, that privacy issues could be a problem, and private-sector alternatives may do the job.

Euro area: tulip-like

The European Central Bank has repeatedly warned about the dangers of investing in digital currencies. Vice president Vitor Constancio said in September that bitcoin isn't a currency, but a "tulip" — alluding to the 17th-century

bubble in the Netherlands. Colleague Benoit Coeure has warned bitcoin's unstable value and links to tax evasion and crime create major risks. President Mario Draghi said this month the impact of digital currencies on the euro-area economy was limited and they posed no threat to central banks' monopoly on money.

China: conditions 'ripe'

China has made it clear: the central bank has full control over cryptocurrencies. With a research team set up in 2014 to develop digital fiat money, the People's Bank of China believes "conditions are ripe" for it to

embrace the technology. But it has cracked down on private digital issuers, banning exchange trading of bitcoin and others. While there's no formal start date for introducing digital currencies, authorities say going digital could help improve payment efficiency and allow more accurate control of currencies.

Japan: study mode

Bank of Japan governor Haruhiko Kuroda said in an October speech that the BOJ has no imminent



plan to issue digital currencies, though it's important to deepen knowledge about them. "Issuing CBDC (central bank digital currency) to the general public is as if a central bank extends the access to its accounts to anyone," Kuroda said. "As such, discussion about CBDC revisits fundamental issues of central banking."

Germany: 'speculative plaything'

In a country where lot of citizens still prefer to pay in cash, the Bundesbank has been particularly wary of the emergence of bitcoin and other virtual currencies.

Board member Carl-Ludwig Thiele said in September bitcoin was "more of a speculative plaything than a form of payment." A shift of deposits into blockchain would disrupt banks' business models and could upend monetary policy, Thiele said. At the same time, the Bundesbank has been actively studying the application of the technology in payment systems.

UK: potential 'revolution'

Bank of England governor Mark Carney has cited cryptocurrencies as part of a potential "revolution" in finance. The central bank started a financial technology accelerator last

year, a Silicon Valley practice to incubate young companies. Carney says technology based on blockchain, the distributed accounting database, shows "great promise" in enabling central banks to strengthen their defences against cyber attack and overhaul the way payments are made between institutions and consumers. He has nevertheless cautioned the BOE is still a long way from creating a digital version of sterling.

France: 'great caution'

Bank of France governor Francois Villeroy de Galhau said in June that French officials "advise great caution with respect to bitcoin because there is no public institution behind it to provide confidence. In history all examples of private currencies ended badly. Bitcoin even has a

dark side — there were this data attacks." He said "those who use Bitcoin today do so at their own risk."

India: not allowed

India's central bank is opposed to cryptocurrencies given that they can be a channel for money laundering and terrorist financing. Nevertheless, the Reserve Bank of India (RBI) has a group studying whether digital currencies backed by global central banks can be used as legal tender. Currently, the use of cryptocurrencies is a violation of foreign-exchange rules.

Brazil: support innovation

The Banco Central do Brasil sees "no immediate risk for the Brazilian financial system" but remains alert to the developments of the usage of those currencies, it said in a statement this month. The bank pledged "to support financial innovation, including new technologies that make the financial system safer and more efficient."

**Canada: asset-like!**

The Bank of Canada's senior deputy governor, Carolyn Wilkins, who is leading research on cryptocurrencies, said in an interview this month that cryptocurrencies

aren't true forms of money. "This is really an asset, or a security, and so it should be treated that way," Wilkins said. As others, she viewed distributed ledger technology as promising for making the financial system more efficient.

South Korea: crime watch

The Bank of Korea's focus has been protecting consumers and preventing cryptocurrencies from being used as a tool of crime. Deputy Governor Shin Ho-soon said this month that more research and monitoring was needed.

**Russia: 'pyramid schemes'**

Russia's central bank has expressed concerns about potential risks from digital currencies, with Governor Elvira Nabiullina saying "we don't legalize pyramid schemes" and "we are totally

opposed to private money, no matter if it is in physical or virtual form." For the moment, the Bank of Russia prefers to delay a decision on regulating the financial instruments unless President Vladimir Putin pushes for action sooner. The central bank will work with prosecutors to block websites that allow retail investors access to bitcoin exchanges, according to Sergey Shvetsov, a deputy governor.

Australia: monitoring closely

The Reserve Bank is closely monitoring the rise of digital currencies and recognizes the technology underpinning bitcoin has the "potential for widespread use in the

financial sector and many other parts of the economy," head of payments policy Tony Richards said last month.

Turkey: important element

Digital currencies may contribute to financial stability if designed well, Turkish Central Bank governor Murat Cetinkaya said in Istanbul earlier this month. Digital currencies pose new risks to central banks, including their control of money supply and price stability, and the transmission of monetary policy, Cetinkaya said. Even so, the Turkish central banker said that digital currencies may be an important element for a cashless economy, and the technologies used can help speed up and make payment systems more efficient.

**Netherlands: most daring**

The Dutch have been among the most daring when it comes to experimenting with digital currencies. Two years ago the central bank created its own cryptocurrency called DNBcoin, for internal circulation only, to better

understand how it works. Presenting the results last year, Ron Berndsen, who was in charge of the project, said blockchain may be "naturally applicable" in the settlement of complex financial transactions.

Scandinavia: exploring options

Like the Dutch, some Nordic authorities have been at the forefront of exploring the idea of digital cash. Sweden's Riksbank, the world's oldest central bank, is probing options including a



digital register-based e-krona, with balances in central-database accounts or with values stored in an app or on a card. The bank says the introduction of an e-krona poses “no major obstacles” to monetary policy.

In an environment of decreasing use of cash, Norway's Norges Bank is looking at possibilities such as individual accounts at the central bank or plastic cards or an app to use for payments, it said in a May report. Denmark has backtracked somewhat from initial enthusiasm, with Deputy Governor Per Callesen last month cautioning against central banks offering digital currencies directly to consumers. One argument is that such direct access to central bank liquidity could contribute to runs on commercial banks in times of crisis.

New Zealand: considering future



The Reserve Bank of New Zealand, once a pioneer on the global stage with its early introduction of an inflation target, said Wednesday it's

considering its future plans for currency issuance, and how digital units may fit into those strategies. “Work is currently underway to assess the future demand for New Zealand fiat currency and to consider whether it would be feasible for the reserve bank to replace the physical currency that currently circulates with a digital alternative,” the RBNZ said in what it termed an analytical note.

Morocco: violating law



Representing one of the more stringent reactions, the country has deemed that all transactions involving virtual currencies as violating exchange regulations and punishable by law.

Cryptocurrencies amount to a hidden payment system, not backed by any institution and involving significant risks for their users, authorities said in a statement this month.

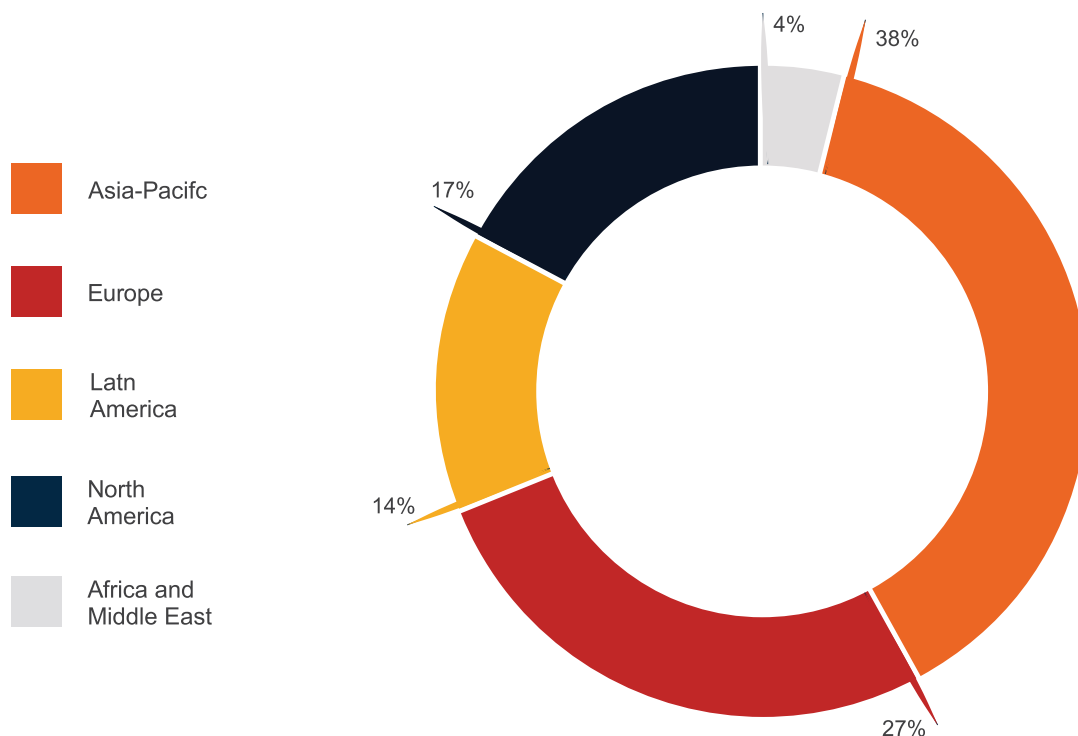
Bank for International Settlements: can't ignore



The central bank for central banks has said that policy makers can't ignore the growth of cryptocurren-

cies and will likely have to consider whether it makes sense for them to issue their own digital currencies at some point. “Bitcoin has gone from being an obscure curiosity to a household name,” the BIS said in September. One option is a currency available to the public, with only the central bank able to issue units that would be directly convertible to cash and reserves. There might be a greater risk of bank runs, however, and commercial lenders might face a shortage of deposits. Privacy could also be a concern. ▶

Cryptocurrency user share by region (based on combined wallet and payment provider data)



5 million preventable
deaths occur every
year



Helpline
1800-11-0456

Reach out to us before
you are one of them

India is keen to work on innovative solutions to promote inclusion, to empower masses and to do so at a faster pace.

Blockchain in India: Moving beyond the rhetoric

Anurag Saxena

IN THE WORLD Economic Forum Annual Meeting, there were a startling range of debates and discussions among the most influential and powerful leaders.

There were differences, and there was the consensus. There was broadly an agreement on the role of technology in driving inclusive development at scale. There was a focussed discussion on emerging technologies including blockchain. This was one theme that was hot in the snow-covered Davos.

Startups, political leaders, think tanks, and industry led the discussions creating a complete chain bringing in consensus that “blockchain is out of beta”.

It cannot be a coincidence that recently even the finance minister of India spoke about blockchain and artificial intelligence in his Budget speech.

India is keen to work on innovative solutions to promote inclusion, to empower masses and to do so at a faster pace. While the resistance to accepting cryptocurrency is quite visible, there has been a lot of action around blockchain in the past year in India.

Almost one year back, India's first blockchain exploration consortium was launched for banks. This was also the time when the Institute for Development and Research in Banking Technology (IDRBT), an arm of the Reserve Bank of India, published a whitepaper on applications of blockchain technology in banking.

NITI Aayog has been encouraging discussions on leveraging technology platforms, and is keen to explore the potential of the blockchain. If we start connecting all the dots, a fertile ground for seeding innovation is ready in India.

With the experience of implementing Aadhaar and India Stack-based applications, we are best prepared to explore if blockchain, artificial intelligence, chatbots, virtual reality and other advanced platforms can be combined to address some of the problems faced by masses. These might include issues related to identity; privacy; food productivity, quality and origin; health advice and the quality and origin of medicines; literacy and numeracy; employment; and ... the list is too long.

This list represents the canvas of opportunities to create scalable solutions to meet a range of the Sustainable Development Goals.

I strongly feel that blockchain or any other technology platform will struggle to solve all these problems while we lack much of the basic infrastructure required. At the same time, potential of such innovative platforms to solve some, if not all, problems of the world cannot be undermined. If a blockchain based platform can help us assess the quality of food grains with complete traceability across the value chain or give the farmer an incentive to share the farm equipment in a community, we are taking some steps towards a larger goal. We are also living in a world which is run by machines.

BLOCKCHAIN



Blockchain also strengthens the application of Internet of Things (IoT) devices by providing a platform for authentication, connection and transaction. The log of all such interactions between devices can be maintained in a secured database. Some of us may stay in a Smart City with a shared pool of renewable energy – smart contracts based on blockchain

could provide a way of optimising the use and efficiency of these (and indeed many other) resources.

Government will play a critical role in ensuring success of blockchain platforms. The ultimate objective of any blockchain platform is to build trust and offer an open, transparent and collaborative platform for users.

Government can provide the vision as well as right regulatory environment, enabling policies and mentorship to nurture the evolution of such platforms.

Dubai is aiming to be world's first blockchain powered government.

According to Smart Dubai, which is conducting government and private organisation workshops to identify services that can be best enhanced by blockchain adoption, the strategy could save 25.1 million man hours, or USD1.5 billion in savings per year for the Emirate. Much of this enhanced productivity will stem from moving to paperless government. Blockchain must be an important link in the Digital India strategy. ▀



You Lead The Change

It is Revolutionary. It is Democratic. It has the potential to transform the economy and share the wealth beyond certain individuals and the corporations. Blockchain can break the monopoly of central banks across the world.

While everyone is talking about blockchain technology, many smart entrepreneurs have already taken the plunge. They are creating innovative systems, products, and platforms which are underpinned by blockchain technology. These startups are utilizing the power of Smart Contracts to make financial transactions more secure, reliable, affordable and instant. With the increased capacity of Bitcoin system, the cryptocurrency is expected to be more inclusive in the future.

The blockchain ecosystem has also brought disruptions in the Fintech sector and expected to bring a paradigm shift in the way companies, and individuals do financial transactions. Top financial institutions including Gladman Sachs have recognized the power of cryptocurrency and have undertaken several initiatives to lead the new phenomena.

MISSION KASHI

our pilot project on Universal Health coverage

**Come & join the movement.
Your Support is important
to us.**

**Register, Donate &
Sponsor at:**

**www.safemedicinesindia.in
or
www.jagograhakjago.com**

Sri Anandamayi Ma
श्री श्री आनंदमयी माँ



24X7 toll free 1800-11-4424

**PATIENT SAFETY AND ACCESS
INITIATIVE OF INDIA FOUNDATION**

a Partnership for Safe Medicines India Initiative

संपूर्ण स्वस्थ कव्रिज . गुणवतपूर्ण स्वस्थसेवा



Is Bitcoin A Waste Of Electricity, Or Something Worse?

A MANUFACTURING START-UP

recently announced plans to move into a shuttered aluminum factory, taking advantage of abundant cheap electricity from the river close by. Instead of smelting aluminum, however, the company plans to turn that power into Bitcoins.

Money is supposed to be a means of buying things. Now, the hottest investment is buying money. While Bitcoin mining may not be labor intensive, it diverts time, energy and capital from other, more productive activities that economists say could fuel faster growth.

"It appears that much of our evolving digital infrastructure is devoted to activities, like the proliferation of cybercoins, that are worse than frivolous," said James McAndrews, the former head of research at the Federal Reserve Bank of New York.

Some economists see evidence that people are playing video games instead of going to work, logging on instead of getting it on, and plowing a growing share of their time, capital and natural resources into virtual products like social media, games and the latest fad: virtual currencies.

Bitcoin, the largest virtual currency, is a particularly voracious consumer of resources because new Bitcoins are distributed in a kind of lottery where each ticket is purchased with electricity.

Bitcoin miners compete for the coins by submitting answers to difficult math problems. Instead of solving the problems, miners use computers to submit a flood of guesses. This can be lucrative: Each Bitcoin is currently valued at about \$10,550.

Believers insist it is a worthwhile endeavor. They describe Bitcoin as a

superior currency that will eventually come into wide use, and they predict even broader applications for blockchains, the digital bookkeeping method used to record ownership of Bitcoins and to verify transactions.

But Bitcoin remains so hard to use that a major Bitcoin conference in January had to stop accepting Bitcoin. It is, in practice, a speculative investment, like gold. And Tyler Cowen, an economist at George Mason University, said mining gold was a better use of resources, because even if it lost value, it could be used to fill teeth.

"Once the Bitcoin power is burned, it is never coming back," he said.

Colin L. Read, the mayor of Plattsburgh, N.Y., also sees it as a public nuisance. The city was guaranteed a fixed supply of cheap electricity as part of the construction



of power-generating dams on the St. Lawrence in the 1950s. Bitcoin mining companies are plugging into that power supply like a swarm of hungry mosquitoes.

Mr. Read said that Bitcoin mining now consumes about 10 percent of the city's power, and that is forcing Plattsburgh to buy a growing amount of extra electricity on the open market, at rates up to 100 times higher than its base cost.

Mr. Read, who is also an economics professor, said he would rather sell the city's supply of cheap power to companies employing large numbers of people. Mold-Rite Plastics, which makes bottle caps, also uses about 10 percent of the city's power, but it employs about 200 people. The mining companies? "They hire a security guard," he said. "And a guy who comes when something breaks."

David Bowman, who describes himself as Plattsburgh's first Bitcoin miner — "I started a long time ago, around 2014," he said — started with a handful of computers. Now he has 20 machines.

A few years ago, he rented a room in an old paper warehouse, where he runs the specialized hard drives around the clock. They sit side-by-side on wire racks, fans whirring to dissipate the heat. About half a dozen other mining companies have since moved into the same building.

Mr. Bowman, who is from Plattsburgh, said he sympathizes with the mayor's concerns. He is the only employee of his company, and he is presently a full-time medical student on the Caribbean island of Grenada. But Bitcoin mining paid his college tuition and it is paying for medical school.

And he doesn't see that Plattsburgh has better options.

"The place needs all the jobs they can get," he said, although his company employs no one beyond him.



Mold-Rite Plastics, a maker of bottle caps in Plattsburgh, N.Y., uses the same amount of electricity as Bitcoin miners, but employs about 200 people.

Credit: Jacob Hannah for The New York Times



Bitcoin companies have begun moving into space at an old paper mill in Plattsburgh, N.Y.

Credit: Jacob Hannah for The New York Times

He does pay fees to an investor-owned company that operates and maintains the machines and has one employee.

Other governments also are grappling with the merits of virtual currencies. Enel, the largest European power company, said earlier this month it would not sell electricity to a virtual miner, citing environmental concerns.

"Enel has undertaken a clear path toward decarbonization and sustainable development and sees the intensive use of energy dedicated to cryptocurrency mining as an unsustainable practice that does not fit with the business model it is pursuing," the company, partly owned by the Italian government, said in a statement.

Some Bitcoin miners emphasize their reliance on renewable energy,

but the energy they use might otherwise be put to other purposes. Consider the example of Quebec, one of the world's largest producers of hydroelectric power. Local demand has flatlined, leading the province to consider exporting electricity to Massachusetts, which is seeking to increase the share of current power consumption generated by sustainable sources. But Quebec is now weighing that possibility alongside a wave of proposals from mining companies.

And plenty of places are hungry for jobs — even the relatively few jobs that virtual mining brings.

Massena, the town with the shuttered smelter, is about two hours from Plattsburgh. It also enjoys a guaranteed supply of cheap electricity, but it has lost several of its major employers, including the smelter and a General Motors factory. ■

**“Let's
Not Fall
Victims
to Fraud
Be Aware”**

JAGOGRAHAKJAGO.COM



10 Incredible Uses For **Cryptocurrency And Blockchain** You Probably Haven't Thought Of

Cryptocurrency to battle election fraud? De-corrupt charities?
Make the world greener? Who knew?



Now, more than ever before is a time to be thinking about cryptocurrencies. Over the past few years, cryptocurrency has grown exponentially because of its attractiveness to people looking to use this alternative money. Bitcoin, the best known of the new cryptocurrencies, is one of those words surrounded by automatic buzz, in part because everyone's so excited about its potential.

CRYPTOCURRENCY, IT TURNS out, has a huge number of uses, many of which will surprise you. Just take a look at these ten:

1. Wealth management

Wealth management is one of the most exciting ways cryptocurrency can be used. That's why companies such as SwissBorg -- a company that's created its own tokens for investment solutions -- are giving investors some great opportunities to manage their wealth without boundaries or restrictions. According to the SwissBorg website, "Whether you are an individual, a DAO [decentralized autonomous organization] or a financial expert, SwissBorg is a democratic ecosystem where you can manage a portfolio of crypto assets."

2. Digital publishing engagement

Digital publishers and advertisers are scrambling to find ways to increase their relevancy with one another. Today, traditional banner ads that have almost nothing to do with an article are simply ineffective with users. To fix the irrelevance problem, SolidOpinion has introduced a new type of pay-per-article advertising where advertisers can pay for valuable ad real estate just above a relevant article that a target audience member is consuming on a publishing site.

This technology utilizes a proprietary form of cryptocurrency, Engagement Token, to fuel engagement; both publishers and audience members can earn tokens by commenting and publishing original content, and advertisers buy tokens to select their ad placements among relevant articles.

3. Ethical business practices

Cryptocurrency can also be used to encourage ethical business practices. Because blockchain makes it possible to track every transaction with complete transparency, businesses with a record of human rights abuses -- the fishing industry, for instance, -- will (hopefully) take on more ethical business practices.

4. Battling electoral fraud

Another ethical application of cryptocurrency will be its ability to help battle electoral fraud. Santiago Siri is the co-founder of Democracy Earth, a non-profit that's designing an app to combine voting with blockchain technology. Siri says that with cryptocurrency, electoral fraud or any other kind of corruption involving money will no longer be possible.

"The blockchain is incorruptible; no one can modify or subvert how the votes are stored, and that's vital for democracy," Siri has said.

5. De-corrupting charities

Additionally, cryptocurrency can be used to avoid corruption in charitable organizations. Because of its ability to keep companies accountable, blockchain can eliminate

many problems occurring with charities, such as fund leaks. That's why the World Food Programme (WFP) is using blockchain to securely distribute cash assistance to the hungry.

6. Going green

If you're an environmentalist, you'll be happy to hear that cryptocurrency can be used to make the world greener, too. For example, there's the Brooklyn Microgrid. With this system, people who already have solar panels are able to sell environmental credits through a phone app, to residents who don't have direct access -- which means using less carbon-based power and more solar-based energy.

7. Travel

As Bitcoin becomes accepted by more and more retailers, people are going to have the chance to use them for a huge number of transactions. Travel transactions are just one category. The website cheapair.com, a travel agency where you can purchase flights, hotels, car rentals and cruises, has been accepting Bitcoin since 2013.

8. Education

More and more, schools are accepting cryptocurrencies as a form of payment. According to Futurism.com, universities in Switzerland, Germany, Cyprus and the United States have started to accept Bitcoin as payment. This form of payment will surely grow as this currency becomes more and more popular.

9. Fund-raising

Many startups are now using cryptocurrencies in order to fund their ideas, services and products. Instead of using traditional VC funding, or using fund-raising websites such as IndieGoGo or Kickstarter, startup leaders are looking to cryptocurrency as a way to raise money for what they need. Because it's easy to track and obtain money this way, it's revolutionizing the entire fund-raising process.

10. Augmented reality

Blendar, rewards users for viewing AR experiences with cryptocurrency. Thanks to the Pokemon Go craze and companies like Candy Lab, which have paved the way for location-based AR, a whole new breed of startups has evolved. Location-based augmented reality experiences will be the future of experiential marketing.

And here, Fluffr.io, is another company to keep your eyes open for, as it has partnered with Blendar and Candy Lab to drive revolutionary in-person experiences, using a social currency based on the blockchain.

As you can see, there are plenty of ways that cryptocurrency is changing every single aspect of our lives. As cryptocurrencies gain popularity in the business world and in our daily lives, more and more uses will come about, revolutionizing the world as we know it. ▶

CONSUMEREXPRESS

Where can consumers have their say about policies and legislation, about their needs and requirements, about products and services, about genuine and fraud companies? We provide you the platform to share with our readers your experiences.
Write to us: pooja@jagograhakjago.com

Vitalik Buterin
inventor of Ethereum



"Blockchain solves the problem of manipulation. When I speak about it in the West, people say they trust Google, Facebook, or their banks. But the rest of the world doesn't trust organizations and corporations that much — I mean Africa, India, the Eastern Europe, or Russia. It's not about the places where people are really rich. Blockchain's opportunities are the highest in the countries that haven't reached that level yet."

Sarah Granger
Author, and Speaker



"While it's still fairly new and unstable relative to the gold standard, cryptocurrency is definitely gaining traction and will most certainly have more normalized uses in the next few years. Right now, in particular, it's increasing in popularity with the post-election market uncertainty. The key will be in making it easy for large-scale adoption (as with anything involving crypto) including developing safeguards and protections for buyers/investors. I expect that within two years, we'll be in a place where people can shove their money under the virtual mattress through cryptocurrency, and they'll know that wherever they go, that money will be there."

Brad Mills
Serial Tech Entrepreneur



"If the trend continues, the average person will not be able to afford to purchase one whole bitcoin in 2 years. As global economies inflate and markets exhibit signs of recession, the world will turn to Bitcoin as a hedge against fiat turmoil and an escape against capital controls. Bitcoin is the way out, and cryptocurrency as a whole is never going away, it's going to grow in use and acceptance as it matures."

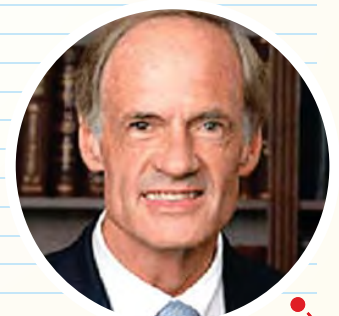


Caleb Chen
London Trust Media

"In the next few years, we are going to see national governments take large steps towards instituting a cashless society where people transact using centralized digital currencies. Simultaneously, the decentralized cryptocurrencies — that some even view as harder money — will see increased use from all sectors."

Erik Voorhees
cryptocurrency entrepreneur

"It is that narrative of human development under which we now have other fights to fight, and I would say in the realm of Bitcoin it is mainly the separation of money and state."



Thomas Carper
US-Senator

"Virtual currencies, perhaps most notably Bitcoin, have captured the imagination of some, struck fear among others, and confused the heck out of the rest of us."



POINTSTONOTE

- The first decentralized cryptocurrency, bitcoin, was created in 2009 by developer Satoshi Nakamoto. It used SHA-256, a cryptographic hash function, as its proof-of-work scheme. It is not known whether the name "Satoshi Nakamoto" is real or a pseudonym, nor whether it represents one person or a group.
- Satoshi Nakamoto, the unknown inventor of Bitcoin, the first and still most important cryptocurrency, never intended to invent a currency. In his announcement of Bitcoin in late 2008, Satoshi said he developed "A Peer-to-Peer Electronic Cash System." His goal was to invent something; many people failed to create before digital cash
- Via Masternodes containing 1000 DASH are held as collateral for "Proof of Service". Through an automated voting mechanism, one Masternode is selected per block and receives 45% of mining rewards.
- Google, Facebook ban cryptocurrency ads
- When the date and time of an event is recorded, we say that it is timestamped. Timestamps are important for keeping records of when information is being exchanged or created or deleted online.
- Bitcoin (BTC) serves as a digital gold standard in the whole cryptocurrency-industry. Other important crypto currencies are Litecoin (LTC), Ethereum (ETH), Zcash (ZEC), Dash, Ripple (XRP) and Monero (XMR).
- In his Budget speech Finance Minister Arun Jaitley stated that the Government of India doesn't recognise cryptocurrencies as legal tenders.
- India's central bank is opposed to cryptocurrencies given that they can be a channel for money laundering and terrorist financing. Nevertheless, the Reserve Bank of India (RBI) has a group studying whether digital currencies backed by global central banks can be used as legal tender. Currently, the use of cryptocurrencies is a violation of foreign-exchange rules.
- As long as a transaction is unconfirmed, it is pending and can be forged. When a transaction is confirmed, it is set in stone. It is no longer forgeable, it can't be reversed, it is part of an immutable record of historical transactions: of the so-called blockchain.
- Only miners can confirm transactions. This is their job in a cryptocurrency-network. They take transactions, stamp them as legit and spread them in the network. After a transaction is confirmed by a miner, every node has to add it to its database. It has become part of the blockchain. For this job, the miners get rewarded with a token of the cryptocurrency, for example with Bitcoins.
- Miners need to invest some work of their computers to qualify for mining. In fact, they have to find a hash – a product of a cryptographic function – that connects the new block with its predecessor. This is called the Proof-of-Work.
- Cryptocurrency and Blockchain may be used to battle election fraud, de-corrupt charities, make the world greener, travel, education, fund-raising and in many other ways in bringing a change to our lives.
- No matter how deep your knowledge base, only use the money you can afford to lose when speculating in cryptocurrencies. ▶

DIGITAL BHARAT. DIGITAL AMWAY.

#ABRUKNANAHINHAI



50,00,000
NEFT transactions
processed to Amway Direct
Sellers in a year



Partnership with ITZ prepaid cards

Forged a partnership with
ITZ prepaid cards six years
ago to digitise cash
transactions



ATM enabled purchases

Bank ATMs enrolled
for Amway product
purchases



95% collections went digital

in November, including
3,00,000 active orders
processed via debit,
credit, ITZ pre-paid cards
& Net Banking

**NACH
PRODUCT**

NACH enabled product purchases

in the North-East



Mandatory KYC

Bank account and
Aadhaar KYC made
mandatory for
appointment as an
Amway Direct Seller



100% digital payments

100% of vendor and
employee payments
happen digitally

Amway India's state-of-the-art
manufacturing facility in Nilakottai, Tamil Nadu.



Join us on facebook@ [/amwayindiaofficial](https://www.facebook.com/amwayindiaofficial) or follow us on twitter@ [/amwayindia](https://twitter.com/amwayindia)

For more details; please visit us at www.amway.in

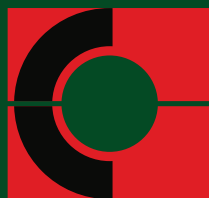
55,000+ HAPPY CONSUMERS

Together WE CAN make a difference



Jagograhakjago.com

Toll free # 1800-11-4424



www.ConsumerOnlineFoundation.org

