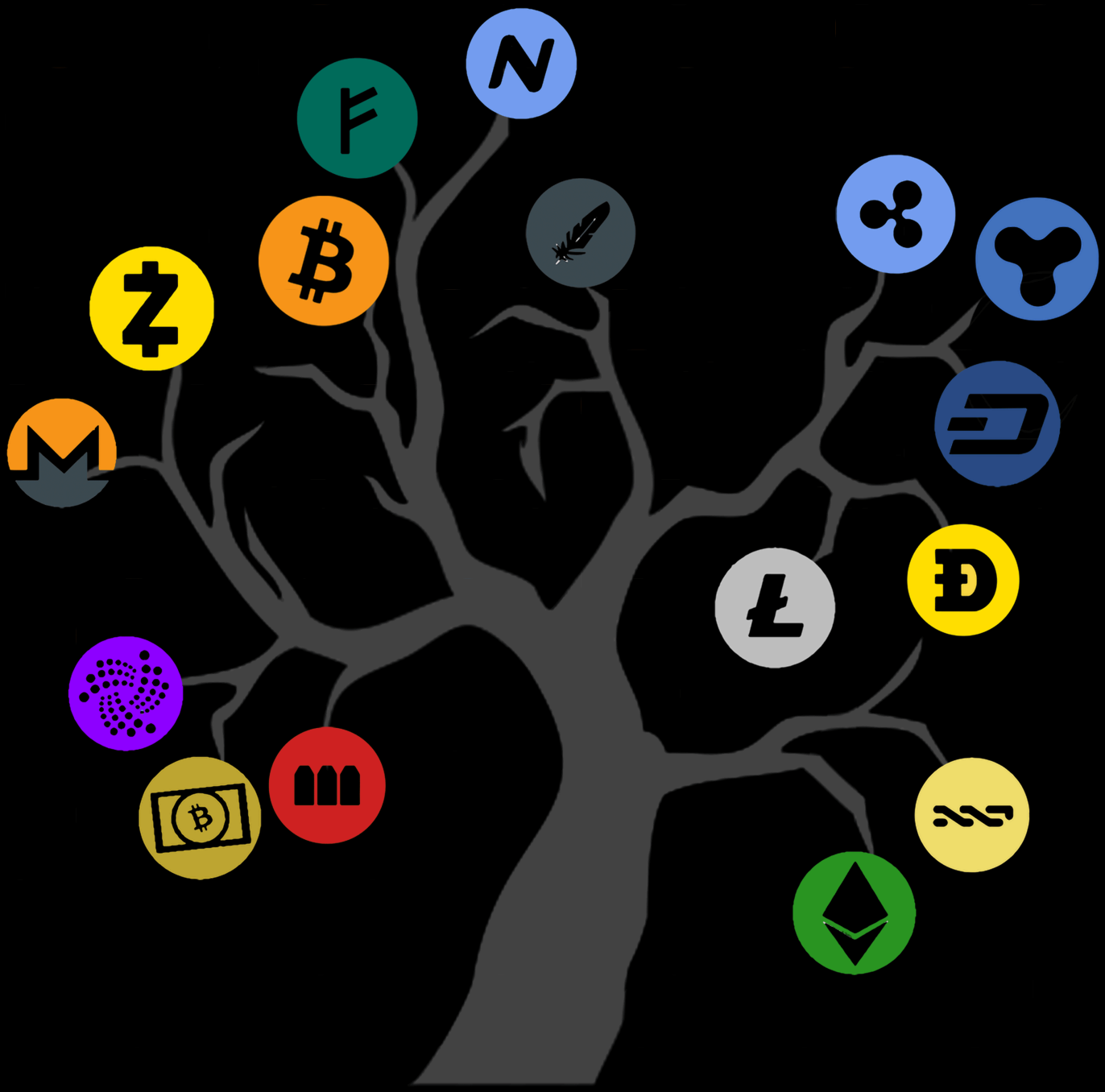
IEEE VESIT

INNOVATION

V.E.S.

AN IEEE-VESIT PUBLICATION



CRYPTOCURRENCY

"IT ALL COMES DOWN TO BINARY CURRENCY"

IEEE VESIT
2017-2018

PRINCIPAL:

DR. (MRS.) J. M. NAIR

VICE PRINCIPAL:

DR. M. VIJAYALAKSHMI

STAFF INCHARGES:

MRS. GRESHA BHATIA
MRS. KAVITA TEWARI

EDITORIAL TEAM:

SENIOR EDITOR

MADHU RAUT

JUNIOR EDITORS

ROHIT KANE
VIGNESH SUBRAMANIAN

DESIGN & PHOTOSHOP

SURAJ BATHIJA

FROM THE EDITOR'S DESK

Dear Reader,

We often hear our co-passengers, shopkeepers, and the commonest of commoners around us, speak about Modi's demonetization and introduction of GST. We, however, have barely heard anyone have enough knowledge about Cryptocurrency, except that one guy in office or college (let's call him Dan), who simply won't shut up about it. In a bid to cater to all the non-Dans out there, IEEE VESIT brings to you, its annual magazine, INNOVATION.

It was an absolute delight, dipping into the articles on Cryptocurrency, sent in for the Article Writing Competition held by IEEE VESIT in 2018. The entries of the first and second prizes for the same have been published in the magazine.

Fiction has always come to man's rescue in the midst of monotonous facts. Some of our council members brought the best out of our theme, in the form of short stories.

Looking at all the YouTube videos and reading articles and books on this exhilarating theme, I realized the need to condense all the concepts in the layman's terms, under one roof. I've elaborated the concept of the blockchain in the cover story, hoping that by the end of it, the reader is equipped with the basic understanding of it.

I can't thank my Editorial team enough for their contributions! I'm grateful to my Junior Editors: Rohit Kane for designing the cover, poster and for his fictional piece, and Vignesh Subramanian for his fictional piece and constant support. I simply can't stop admiring the efforts our SE Coordinator, Suraj Bathija has put in making literally every page of this magazine possible!

The true success of this magazine, can be measured in terms of the buzz created around Cryptocurrency after reading it. We hope we've cultivated enough utopian enthusiasm in you.

My best wishes, always! Happy reading!

Madhu Raut
Senior Editor, IEEE VESIT

Satoshi by Juan Miguel Delgado

Source: https://goo.gl/2fpxDo

This poignant portrayal of a bitcoin transaction depicts a homeless beggar accepting a donation from a purposely faceless man--presumably Satoshi Nakamoto. According to the artist, a Costa Rican man named Juan Miguel Delgado, the beggar is supposedly a former banking executive. The QR code in the painting directs to a real wallet address that claims to be used to donate to the poor.

Scan for more information on this topic:

CONTENTS

THE CRYPTO WARFARE 1
By Sakshi Patil

4 A BEGINNERS GUIDE TO CRYPTOCURRENCY
By Krithika Srinivasan

END OF THE ROAD 6
By Mukul Sharma

7 DECRYPTING CRYPTOCURRENCY
By Rohit Sreedhar

BITCOIN 2040: AN ORWELLIAN TALE 8
By Vignesh Subramanian

10 CRYPTOCURRENCY: BOON OR BANE
By Lairai Karnik

THE CONUNDRUM 12
By Takshan Shetty

14 CRYPTOCURRENCY
By Pratik Bhatia

THE SATOSHI DICE 15
By Madhu Raut

23 VIRTUAL PRETENCE
By Rohit Kane

CRYPTOCURRENCY 25
By Juyee Sabade

27 THE BITCOIN MIRACLE
By Yash Marathe

CRYPTOCURRENCY 29
By Dhaval Bagal

30 THE TRUEST CURRENCY
By Hitesh Jetwani

THE CRYPTO WARFARE

By Sakshi Patil
(Executive Committee, IEEE VESIT)

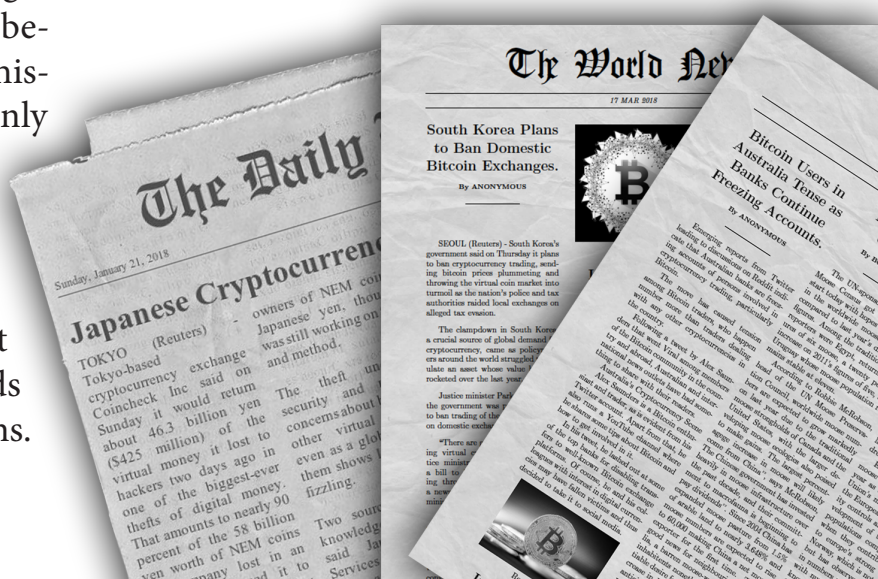
January, 2018.

12-year-old Jamal frowned at the computer screen, biting his lower lip. There was a hush in little room filled with computers, even as the market outside was filled with hustle. None of the 15 people in that room had anticipated the fall of cryptocurrency this soon. However, what nagged Jamal the most was that his calculations had failed, and they never did. Well he was precocious, that coupled with an endless curiosity made him nothing short of a child prodigy. By 12 he had become a master programmer, developer and a hacker, now with a linking motif of becoming a jack of all cryptocurrencies.

The year 2017 had been hailed as the breakout year for the cryptocurrency industry and it was during this time that most virtual currencies made a dent in the markets. However, by the end of 2017, every other cryptocurrency had suffered significant losses which registered by the world's best performing cryptocurrencies had amounted to a sickening $100 billion (USD). The ruling mechanism of the cryptocurrencies were their blockchains. When a transaction is confirmed, it is set in stone & no longer forgeable. It couldn't be reversed and became a part of an immutable record of historical transactions: of the blockchain. Only miners could confirm transactions & principally anybody could be a miner. Since a decentralized network had no authority to delegate this task, a cryptocurrency needed mechanism to prevent one ruling party from creating thousands of peers and spreading forged transactions.

That's exactly what 10 out of the 15-people sitting in an attic in Afghanistan had done; vitiated the fundamentals of cryptocurrency. Now there were 10 miners in this room everyone with their own blockchain, on the verge of either losing all the 2.5 million dollars they had accumulated or worse stagnate their mission. Jamal elucidated that if there are people who could track down the investors in a blockchain and notify the world governments, they had powerful backing.

He was right. Except it wasn't people, it was Lieutenant Jack Hobbs. Lieutenant Jack Hobbs was a cryptologist who worked for the navy, Department of defence (DOD), long before he fell in love with linguistics and mathematics. The government now valued him more for his cryptology skills rather than his sailing prowess. He believed that cryptocurrencies are responsible for deaths because they allow online drug transactions and had a presage that criminals, terrorists and tax evaders could be using it for their benefit because of the anonymous transactions they allow. That reputation grew when it became the sole currency accepted on Silk Road, the Dark Web marketplace for drugs and other illicit goods and services. No sooner did he had the chance to present this in the UN general assembly downfall of cryptocurrency became evident. But he knew this wasn't the end.



Monero was invented to add the privacy features which were missing from other cryptocurrencies. 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, Monero's kryptonite algorithm was able to cut through that trail. Monero 's popularity peaked darknet markets decided to accept it as a currency. This resulted in a steady increase in the price, but the actual usage of Monero seemed to remain disappointingly small.

Back in Afghanistan, Jamal and his team decided to expand their resources and make Monero a huge hit. Their plan worked as Monero's popularity peaked globally, privacy guaranteed. This was their revenge, in the face of Amrikis whose air strikes in the anti-IS operation had killed thousands of innocent people; made Jamal an orphan before his uncle adopted him. At the age of 10, made the world of web his stage. Now they planned to start an organization with the money, resources and weapons to protect the innocent people during these airstrikes.
A slap in the face of all his dedication Jack Hobbs desperately spent his days trying to get into the system using transaction malleability. The blockchain was created to be completely immutable, which it achieved through cryptographic hash functions. What this essentially means is that once data has been put inside the blockchain you cannot tamper with it. Just this quality alone gives blockchain based cryptocurrencies immense security. However. turns out that the signature that goes along with the input data can be manipulated, which in turn can change the transaction ID. In fact, it can make it seem like the transaction didn't even happen in the first place.

Hobbs's move became a game changer and transaction malleability a success. He was invited to head a mission which had been known and approbated only by the Government's chosen few. America had already anticipated the onslaught of a nuclear war and embarked on a spree of securing allies. They needed lands to harness and store the nuclear weapon harmful to their own citizens. A genius idea from a shrewd captain that the cryptocurrencies be used to hack and steal the money from illegal organizations to aid third world countries, rehabilitate them only to ensure the sacrifice of their lands and lives during the war; raise them like a pig for slaughter. Jack Hobbs was appalled and was torn between honouring his duty towards his country or saving the humanity.

FUN FACT!

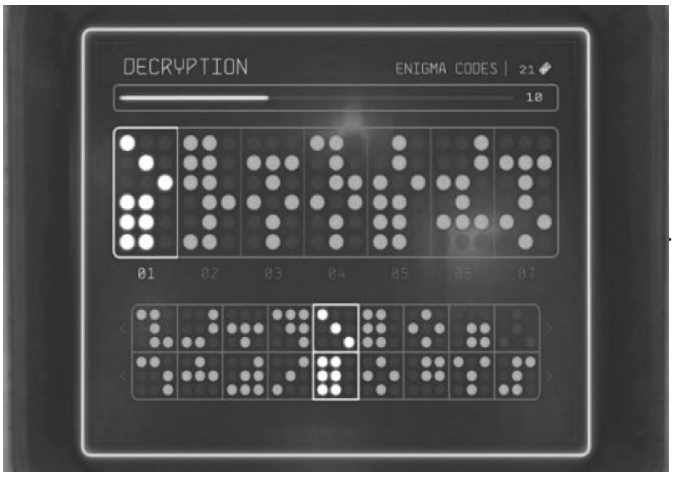
Did You Know?

You can see every transaction that has ever been made on **Bitcoin**.

You just won't know all of the details about the parties involved, Because there is **No Centralised Institution**.

The information is **publically accessible**.

Next night, what could be called a fortuitous moment, he received a modern-day version of enigma code, representing parts of a code that, when combined with other segments of the code, can be used to decipher the original code.



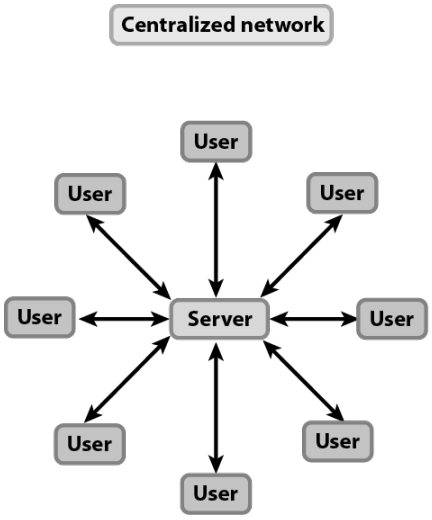
December, 2019.

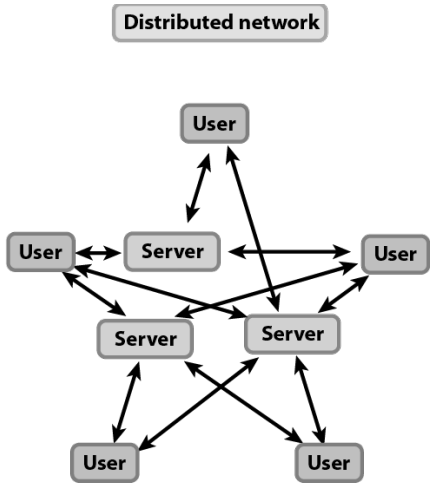
World wide web was in a frenzy. All the traces of cryptocurrencies had vanished into thin air. For the past whole two geniuses had worked together to erase the blockchains, forced ICOs to initiate cash outs and simply created a virus that crashed the entire networks on the websites. The internet was flooded with the mystery case of vanishing lieutenant who had managed to erase his existence from all the databases globally. And one fine day, in the year 2050, Jamal who now headed the Democratic Youth Organization of Afghanistan, received an enigma code, with the key to revival of the first blockchain in 20 years and a single message.
"It's Time."

Questions & Answers!

Simple Answers to common Questions.

What is the basic difference between a Centralised & a Distributed Network?





The Cryptocurrencies are a great example of the **Distributed network**.

The fact that there is **No Central Network**, makes it safer & offers **Anonimity.**

A BEGINNER'S GUIDE TO CRYPTOCURRENCY

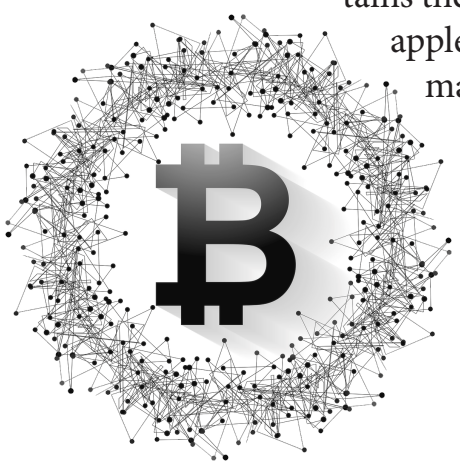
BY A BEGINNER

By Krithika Srinivasan, D20
(BE, First Prize)

SO, WHAT IS A CRYPTOCURRENCY?

At its very essence, it's a decentralized cash system. Digital cash systems present problems that physical systems or systems based on them do not have. Let's consider the following example: Suppose we're sitting on a bench, and I give you an apple. This transaction is relatively straightforward. Before, I had one apple and you had none. After I gave you the apple, you have one apple and I have none. This is something that you can see. Now let's alter the scenario by imagining that I give you a digital apple. Now this transaction is not something you can see. You now have one virtual apple, but how do you know that I now have zero? Can you be sure that I haven't made copies of my one apple and kept them all to myself? Or given them to other people?

This is a problem that economists call Double Spending and is a problem that all virtual currencies before the Bitcoin faced and was the reason they failed. So, what makes Bitcoin different? The most important part of Satoshi Nakomoto's, (the inventor of the Bitcoin) invention was that he managed to build a decentralized digital cash system. To continue with our example of digital apples, imagine that there's a ledger that maintains the number of digital apples, who has how many and all the transactions that take place. Would that solve the problem? Not exactly, because the person with the ledger might still be able to fudge numbers and update the ledger to fool everyone else. But what if everyone has the same ledger? This is what makes the cash system decentralized. Instead of one server managing accounts, balances and transactions, every entity in the network does it. You won't be able to perform 'illegal' transactions because then it wouldn't sync up with the ledger.



HOW DOES IT WORK?

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. 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 must 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.

WHAT'S THE FUTURE LIKE FOR CRYPTOCURRENCIES?

Cryptocurrencies are still in their infancy. Dozens of cryptocurrencies are invented every year. Early adopters of these currencies hope to get rich. Most of them fail and investors lose money. Established cryptocurrencies like Bitcoin, however, are probably here to stay.

The next couple of years for these currencies however, will not be smooth-sailing. Economists claim that due to the complete lack of a regulatory body, people may be buying so much bitcoin that it might lead to that bubble bursting, causing a crash in the value. Warren Buffet, the famous investor, says "Bitcoin and cryptocurrencies will come to a bad end". Aside from all this naysaying and doom-and-gloom, many established banks have begun banning the purchase of Bitcoins with their credit cards. The European Union is also threatening to regulate Bitcoins unless the risks are not tackled.

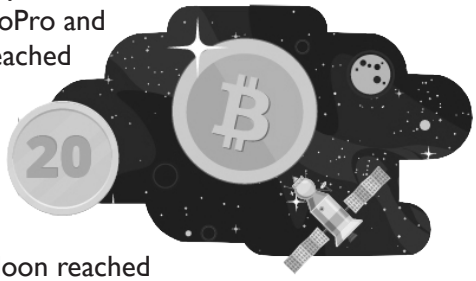
So, are cryptocurrencies the way of the future? A digital currency for the digital age? Or will its very defining trait, its decentralized nature be its downfall? Only time will tell.

FUN FACT!

Did You Know?

Bitcoin has been sent to space!

Genesis mining sent Bitcoin to space. They sent a 3D Model along with a Bitcoin paper wallet, which were tied to a weather balloon and released. The journey was recorded using a GoPro and once the balloon reached 20 Kilometres, the ground team made the transaction to paper wallet. Another transfer was made when the balloon reached 34 Kilometres.



"Bitcoin is exciting because it shows how cheap it can be. Bitcoin is better than currency in that you don't have to be physically in the same place and, of course, for large transactions, currency can get pretty inconvenient."

- Bill Gates, Co-founder of Microsoft

Questions & Answers!

1. What are the accepted Bitcoin Tickers/ currency codes?

a. BTC or BIT
b. BIT or XBT
c. BCN or LTC
d. BTC or XBT

2. Who invented the Bitcoin?

a. Donald Trump
b. The CIA
c. Satoshi Nakamoto
d. Mark Andersen

3. Which famous Boxer owns a Bitcoin ATM/

a. Vladimir Klitschko
b. Vitali Klitschko
c. David Haye
d. Mike Tyson

4. How does the Bitcoin Protocol Work?

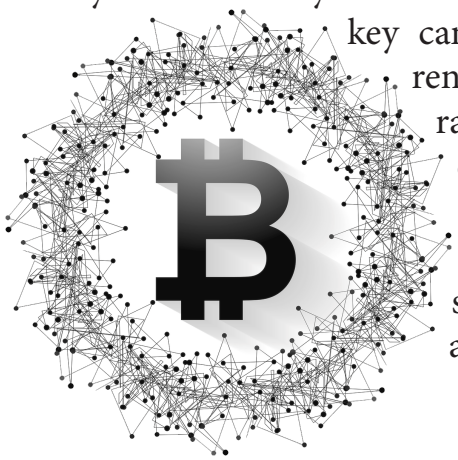
a. It's centralised
b. It's decentralised
c. It's owned by Bitcoin Foundation
d. Skynet

1-d, 2-c, 3-d, 4-b

END OF THE ROAD

By Mukul Sharma
(Executive Officer, IEEE VESIT)

Every story has a beginning and an end. However this is not one to follow the norms of spinning a yarn. This story may never end. It was a warm summer evening in Kansas City, Missouri. The farmlands rich with the sound of dried up leaves rubbing against the farmers boots, and the subtle, musical tones of his cattle's cries waning away as dusk approached. Young Ross Ulbricht stood outside the farmhouse intently listening to the last of his fathers story of a magical, yet not far from reality, tale of a Silk Road. "The silk roads were an ancient trade route", said the farmer while wiping his brow, " they helped merchants fend for themselves and make an honest living". The farmers tale was gripping to say the least. His words resonated within the confines of the young boys mind and with that, he went on to become a pioneer to some, but a criminal to many. He was the owner of the worlds largest "Silk Road", a part of the Internet that supplied drugs based on order, that poisoned many with the ruse of a temporary buzz, and most nefariously, robbed the patrons of any crypto currency they had acquired. 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. Yet this man had figured out the secret to extract Bitcoins from a fund. Any visitor on his site would experience a certain glitch that would crash the computer, severing the link between the server and client on the clients end, but maintaining direct access to the clients crypto currency funds. From this he could gain all the money that he needed and would leave untraced. Ross felt like a god. Nobody could touch him for he could not be accused of stealing that which may not hold any physical value with all certainty. However, Ross did not account for the fact that one day he would steal from the wrong patron. Cecelia Hemingsworth was an ethical hacker in need of some medicinal refreshments, who happened to stumble upon the Silk Road and its glitch inducing code. Through some use of wit and acquired skill, she managed to retrieve not only her accumulated sum, but also that of many others. What she did beyond that is unknown but Ross got what he deserved. He was arrested on multiple counts and Silk Road was no more , and Cecelia moved on from that incident with a new understanding of the rapacious nature of certain individuals.



The Crypto-Currency Community hasn't decided whether they want to be anarchist rebels or replace the establishment.

- Adi Shamir

FUN FACT!

Did You Know?

The inventor of Bitcoin is still unknown.

Since the inception of Bitcoin in 2009, there have been several speculations about who the father of Bitcoin is.

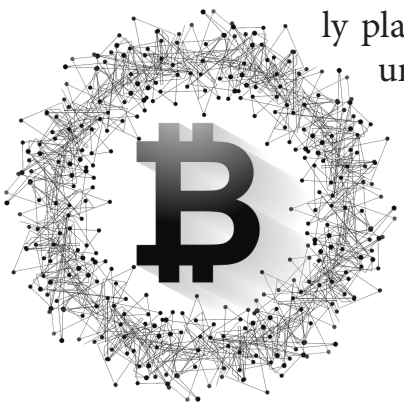
The Bitcoin whitepaper was made open to the public under the pseudonym of Satoshi Nakamoto. The identity of "Satoshi" is still a mystery yet to be solved.

DECRYPTING CRYPTOCURRENCY

By Rohit Sreedhar, D19A
(BE, Second Prize)

Imagine your television sets and mobile phones alarmingly breaking out the news of yet another avatar of the current currency, while rendering your lockers redundant. And you, instead of biting your nails at the ATM queues, are chilling with your favorite book. Yes of course banking over the internet and stacking up money on a piece of plastic has facilitated cashless dealings for quite a while. But hey! You are still functioning under a centralized authority that governs the valuation of your stakes. Before you begin to believe that I'm suitably endorsing the need for the resurrection of the monetary hierarchy, let's take a moment to appreciate the emergence of system that has given so much of fluidity and seamlessness to the most fundamental aspect of our existence today, money. Crypto currency platforms your funds on a dynamic forum, wherein you are equipped to play your fair share of the game while being encrypted! The deals which could be sealed are being written on the constantly widening horizon right from retailing to paying fees. Also, you could use this to stock up your ammunition, just in case you are planning a shoot out!

Cryptocurrency, in its various forms, ensures the conformance of transactions as well as the storage of money. So, while Gucci is painstakingly stitching its exclusive wallets, a hard drive is unassumingly playing the digital treasure. Gliding along the concatenated giant, block chain, cryptocurrency makes its way from the sender to the receiver. Accoutered with the army of a hash code, encryption details of the previous data and finally the lead data, a block fits itself into a propagation which eventually seals the deal. Picture in your mind a gamble, wherein each gambler minutely chalks out the gains and losses of all his counterparts to ensure that no one is tricking on the other. This is exactly how this system ensures the avoidance of discrepancies without the watch of a central authority, with the maintenance of a ledger by each stake holder. Each of these ledgers are then awarded points that bulk up the profiles of the ones who maintain them. Who'd thought real life monopoly would be a game changer!



Cryptocurrency is backed by flexibility and anonymity but is it truly that strong to overturn the existing financial decorum? Anonymity is surely a step that preserves your confidentiality, but it as well is a loophole that secretly feeds smuggling. Illegal activities anyway sneak their way out right under the nose of a transparent system and granting them this veil only shows them an easier door. Bill Gates quotes that cryptocurrency is in a way killing the world by making it easier for drugs to land in our hands. It truly is and so is it for every such malpractice, but I'd like to believe that the system that can change the face of something as structural as money has yet more faces in store to make the world a better place.

Bitcoin 2040: An Orwellian Tale

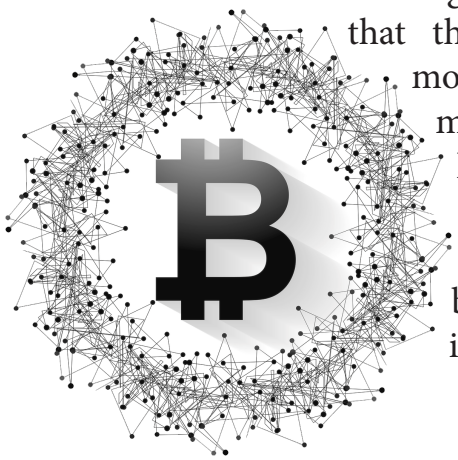
By Vignesh Subramanian
(Jr. Editor, IEEE Vesit)

Have you heard of the Rothschild family? You probably know them only in some (growing) conspiracy theories. If this journal finds you in time, that is.

Hi there, I'm Alan Wayne, one of the first bitcoin snatchers - bitcoin miners who found a way to successfully mine even after they had apparently "dried out" back in '25. How I wish I hadn't done that though. Because now, in the year 2040, when major economies have made the leap to bitcoin, the world sees it as the messiah that will finally lead them to Utopia. But, as I have recently discovered, and may face dire consequences for doing so, this messiah is an impostor, not very unlike the Pied Piper, leading us mesmerized rats to the depths of a dystopian ocean. Bitcoin is nothing but a massive bait, ready to capture mankind in its entirety in one single, fluent motion.

> *Bitcoin is not a currency for a Government;*
> *It is a global currency for the people.*
>
> **- Wences Casares**

Back in 2025 when the bitcoin count reached its limit, some of the leading bitcoin miners, including me, tried finding ways to access the ledger, to create more bitcoins. Two years passed before four of us stumbled upon a hidden backdoor into the ledger, through which we entered the ledger, and discovered that the ledger allowed more bitcoins to be mined, although in limited quantities at a time. The already massively blown out popularity of bitcoins practically exploded, as more and more people started putting their trust in bitcoin, as even governments started to accept bitcoin as legal tender. However, I started feeling a bit unsettled. How didn't we discover this door earlier? How did we discover it now? A few days of constantly monitoring this back door and I hit pay dirt. An unknown person accessed the backdoor. I assumed that it maybe was a new person discovering it, until he started making changes to the goddamn ledger itself. At that instant I knew this was no newbie. This person had discovered the backdoor way before we had. He/she probably had created this backdoor. With a sinking feeling in my stomach, I realized maybe this person created the ledger itself. A quick search revealed an IP address located somewhere in Korea. Fake. Very secure. But not enough. I traced the original IP in a few minutes and punched in a few commands to retrieve its owner's name. After what seemed like an eternity of watching the terminal's cursor blink, a name appeared on the console which made me forget how to breathe. Nathaniel Rothschild.



FUN FACT!

Did You Know?

The Silk Road was a way for internet users to order illegal drugs anonymously, and the first major place that **Bitcoins** were used.

Bitcoin was one of the major reasons that **The Silk Road was so successful**, and lasted as long as it did before it was shut down in **2013**.

I woke up to the cacophony of magpies perched somewhere above me. It's been six months since I fled my one room studio, but I knew I was no further away from them as when I had started my run. Them being the Rothschilds, hot on my trail since the day I found out they owned almost half the governments. It had all been a sham, the world wars, the cold war, the space race, all vying for the public's attention, while the greatest conspiracy of all time was working smoothly and silently behind the scenes.

And bitcoin was the final move in this coup. The ledger was created by the Rothschilds, using an anagram of Nell Tomoka Rothschild's middle name along with Nathaniel's first syllable to create the name 'Nakamoto', making sure it sounded as far away from them as possible, adding the Oriental sounding 'Satoshi' for good measure. They owned the ledger, they created the backdoor we found, they made everyone switch to it, fall for it, and they've now practically finished the game.

They've found me.

Its three am on my alarm clock, and I'm writing this (possibly)last entry in the hope that someone will find this and realize the danger before it's too late. They can access the ledger anytime and set whatever price they want. Entire economies will fall, begging them for mercy, and those who haven't made the switch to bitcoins will have no chance against the army that they would command. This needs to be stopped, as soon as possible. Below I'm going to give the details of how to access the ledger. Follow it carefully, and sto--

CRYPTOCURRENCY: BOON OR BANE

By Lairai Karnik, D11B
(TE, First Prize)

Bitcoin. Block chain. Mining. Ledger wallet. Well, these are the buzzwords floating around a lot lately. All of us are quite conversant with the fact that these fall under a greater umbrella-the mother of all buzzwords currently trending-Cryptocurrency. But, what exactly is cryptocurrency? Is it as exciting and promising as it is made out to be, or simply a passing fad, only to be forgotten in the course of time? Well, simply put, cryptocurrency is a digital or virtual currency that uses cryptography for security. Though Bitcoin, or 'virtual gold' is indisputably the most popular one, launched in 2009 by an unknown person under the pseudonym Satoshi Nakamoto, its success spawned several competing cryptocurrencies, such as Litecoin, Namecoin and PPCoin. The three prime aspects of cryptocurrency are decentralisation, anonymity and immutability. Decentralisation refers to the absence of any centralised authority to regulate it. All the transactions, financial activities maintain anonymity. So, you don't know whom you're co-operating or dealing with, which is why staunch supporters of cryptocurrency often highlight that it's all about good faith and that anonymity is essential to preserve the very nature of cryptocurrency. Lastly, immutability is nothing but the property due to which data once stored cannot be changed or erased.

The irony lies in the fact that these aspects that embody cryptocurrency bring with them a plethora of advantages as well as disadvantages. While decentralisation renders Bitcoin free from government manipulation or interference, the flipside is that there is no central authority to back the value of a Bitcoin or to ensure that things run smoothly.

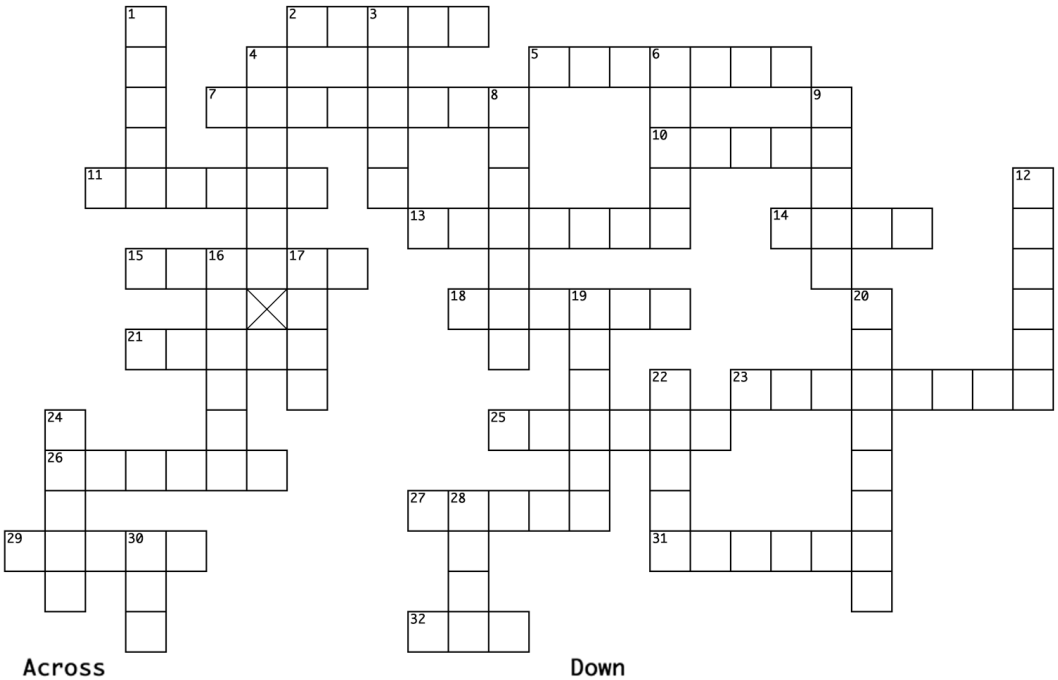
Such characteristics make Bitcoin fundamentally different from conventional currencies, which are backed by the full faith and credit of their governments. It is no news that Bitcoin's major benefits-decentralisation and anonymity have also made it the currency of choice for a host of illegal activities such as money laundering, drug peddling, smuggling and weapons procurement, which has inevitably attracted the attention of powerful regulatory authorities and other government agencies.

In May 2013, the DHS froze an account of Mt. Gox-the largest Bitcoin exchange-alleging that it broke anti-money laundering laws. Also, in August, New York's Department of Financial Services issued subpoenas to 22 emerging payment companies, many of which handled Bitcoin, asking about their measures to prevent money laundering and ensure consumer protection. These instances aptly portray how the success and growing visibility of cryptocurrencies is proving counter-productive for them-the more popular they become, the more regulation and government scrutiny they are likely to attract.

There are other limitations too that cryptocurrencies presently face such as people maintaining multiple identities on a single network, energy wastage as well as the possibility that one's digital fortune can be erased by a computer crash, or that a virtual vault may be ransacked by a hacker. However, I believe such limitations can be overcome with technological advances. In my opinion, the beauty of cryptocurrency lies in how its prime aspects are intertwined with each other. Anonymity is pivotal in maintaining decentralisation and if we compromise on these core characteristics that define cryptocurrencies, to curb nefarious activities, it will destroy the very premise of their existence.

Moreover, the problem of untraceability, for which cryptocurrencies are criticised, exists to a great extent in the case of cash as well. In fact, it is still widely used for illegal activities and large-scale scams, without banks being able to bring this under control. By no means do I think that cryptocurrency is a boon. All I wish to convey is that it is neither a bane. It cannot be labelled as completely white or black, but it exists in a grey zone with substantial opportunities and scope to become as ubiquitous as dollars and euros in the near future, coupled with its own set of risks. So, all in all, I believe cryptocurrency is definitely here to stay.

CRYPTOCURRENCY CROSSWORD



Across

2 Birdwatcher
5 Digital gold
7 Full of people
10 Very close
11 Fastener
13 Band material
14 Not one ___
15 Type of dragon
18 Disturbance
21 Flight tools
23 Squeeze these
25 Digital gold, to the Dutch
26 Brian Eno song
27 Passion
29 Put the pedal to it
31 Standing
32 Took the red pill

Down

1 Good feeling, to a Norwegian
3 Brought to life
4 Coin, to Zamenhof
6 Japanese car
8 Cake components, to a Catholic
9 Pepo
12 Knowledge, to a Hellenist
16 Typeface
17 Get there quickly
19 Roof holder
20 Blunt
22 Connection
24 Surfboard holders
28 What Jesus did on the third day
30 Where the animals went

*all answers are names of cryptocurrencies

THE CONUNDRUM

By Takshan Shetty
(ExeCom, IEEE VESIT)

Day 1:

Tryst, being one of Mumbai's five-star clubs, was home to the affluent societies of the western suburbs. Kabir Oberoi was one of the frequent visitors. On that night, Kabir was at Tryst, like every other Saturday. While sipping the drink with his pals, the glass fell to the ground and so did Kabir's body. Scared and panicked, his friends rushed him to the hospital, but it was too late, he had already died, supposedly of a heart attack. But the doctor noticed something unusual, he was boiling with fever minutes before he took his last breath. So, on the doctor's advice, his family decided to go to the police.Being a high-profile case, one of the top officers, Mr. Jadhav was on the case. There was political as well as media's pressure on the police department, so Jadhav was pressurized to get more than satisfactory results in 5 days. The investigation began.

Day 2:

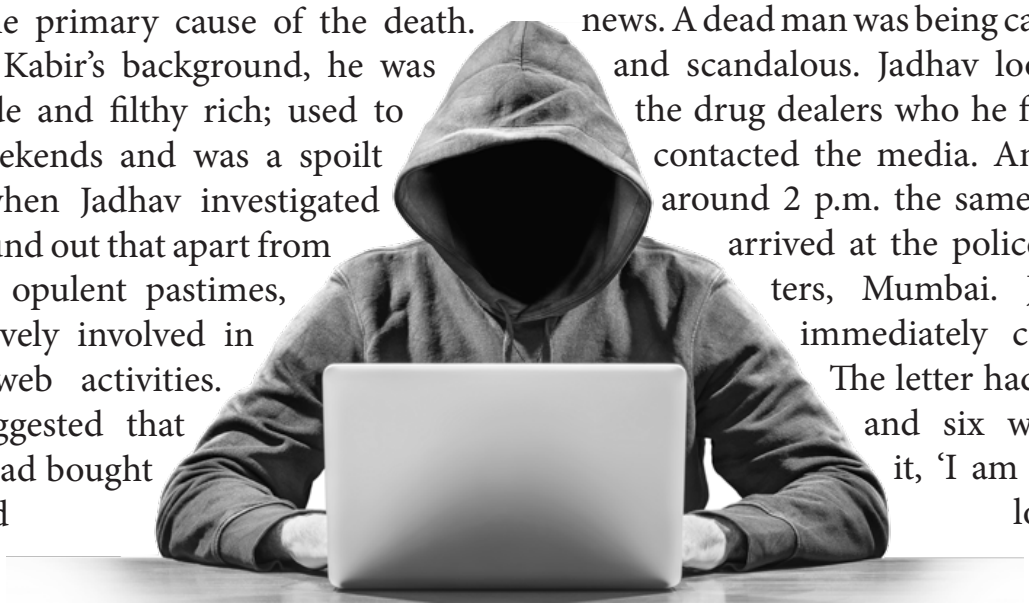
Jadhav started with looking at the forensics report which stated heavy involvement of MDMA in the victim's blood. This was declared as the primary cause of the death. Looking at Kabir's background, he was young, crude and filthy rich; used to party at weekends and was a spoilt brat. But when Jadhav investigated more, he found out that apart from the general opulent pastimes, he was actively involved in the deep web activities. Reports suggested that the victim had bought arms and drugs in the last two years which suggested his interest and involvement in bitcoins. He also had a team of techies who dealt with all the digital currency related activities. This was a big lead to something not so very common in this case.

Day 3:

The police could not capitalize on this lead, as all the digital transactions were done via bitcoins. The address of the sellers could not be traced. To get closer to this, the police hired latest tech geniuses to get their hold over the dark web, but tracing the seller was just not possible. Jadhav wasn't even sure if he was going down the right path, he started doubting himself. So, he went back to interrogating Kabir's family and friends; but Jadhav had already got everything out of them. Just when the case seemed out of reach, a report from the lab arrived which stated that the MDMA in Kabir's body had excess traces of nitrogen, which was responsible for the sudden collapse of the victim. This made the supplier of the drug the prime suspect in this case.

Day 4:

The next morning, the victim was all over the news. A dead man was being called corrupt and scandalous. Jadhav looked for all the drug dealers who he felt would've contacted the media. Amongst this, around 2 p.m. the same day, a post arrived at the police headquarters, Mumbai. Jadhav was immediately called there. The letter had an address and six words below it, 'I am what you're looking for.'



The police rushed to the given address where they found another letter which had a list of scams under the victim's name, including smuggling drugs without counter payment for months. The suspect ended the letter with a casual tease for the police to not look for him, as he's leaving the country soon. Jadhav ordered all the trains and flights to stop going out of the country. He rushed to the Mumbai airport and checked every boarding passenger's details himself. Whilst he was at the airport he received a phone call from an unknown number. A young and conquest voice said, "Sir, I liked the waves in the ocean more than the stars in the sky."

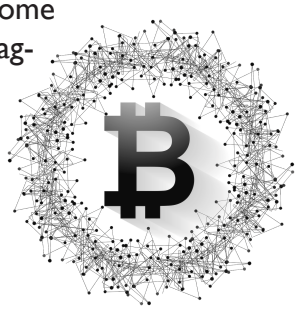
A 5 day case was lost in 4 days.

FUN FACT!

Did You Know?

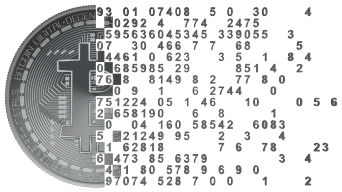
Bitcoin is an open-source software, which means anyone and everyone who does not own it, can access it.

The same way you connect to some website and download some images or songs, the same way you can get the Bitcoin.



Also, no company stands behind the creation of Bitcoin, thus, since the creator is anonymous, there is no owner.

Crypto-Currency Puzzle



E	H	A	C	K	E	R	Z	N	C	M	D	V	H	X	U	D	R	C	P
W	C	D	L	A	T	I	G	I	D	S	U	K	M	D	P	C	L	O	Q
B	I	N	P	Q	K	W	S	O	D	I	B	O	U	Y	M	V	U	X	W
W	I	R	A	V	J	P	Q	C	Y	J	Y	V	W	I	F	T	Z	R	M
K	C	M	U	N	P	N	L	T	K	P	S	H	A	E	X	R	A	B	D
K	Y	B	O	P	I	K	W	L	V	E	S	I	C	B	Z	F	I	C	P
X	Z	M	A	K	N	F	Z	A	E	C	X	H	G	Y	Q	T	U	D	L
J	H	Z	F	M	Z	X	C	M	O	U	H	M	G	N	C	X	K	D	T
F	D	B	C	O	M	B	D	Y	K	R	C	A	Z	O	A	O	A	E	H
B	F	J	M	E	D	K	M	D	B	R	J	J	I	T	P	T	G	N	R
B	L	O	C	K	C	H	A	I	N	E	U	N	P	T	M	R	U	E	W
T	G	L	E	U	K	H	Z	N	D	N	R	S	Y	D	I	U	B	R	X
Z	J	H	O	E	T	P	M	B	M	C	T	R	I	L	N	D	L	E	E
F	Y	W	V	Y	X	W	K	Q	S	Y	C	C	Z	R	E	D	T	O	C
A	A	G	T	B	Z	G	M	V	W	H	O	I	J	G	R	H	B	K	V

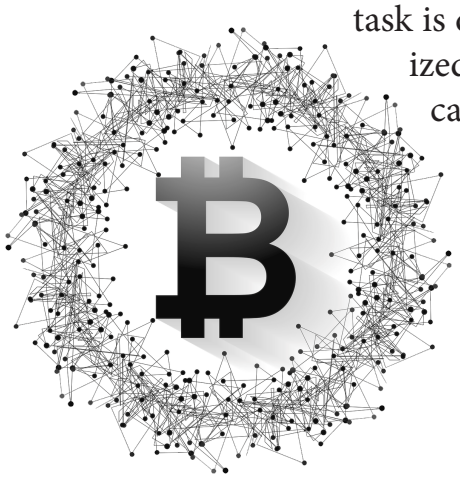
Solution:

ALTCOIN
CRYPTO
DIGITAL
BITCOIN
CURRENCY
FINANCE
BLOCKCHAIN
CYBER
HACKER
SIGNATURE
MINER
ICO

CRYPTOCURRENCY

By Pratik Bhatia
(TE, Second Prize)

Agreeing with one famous US senator, cryptocurrency has captured the imagination of some, struck fear among others and confused the heck out of the rest of us. Being one of the confused crowd, helps you to ignore the topic as a whole. Until you come across a simpler explanation of same topic that ends you up in the imagination crowd. A coin of neither gold nor any precious metal and additionally you will never stumble upon anything of this sort or steal from someone, simply because it is a digital currency that exists electronically only. What makes it stand apart from any other currency is the simple fact that it isn't governed by any central issuing authority or any regulatory body. No detection of fraud or no keeping tracks of where they are, or no production count maintenance are the few attention-grabbing advantages one must wonder about. It is a completely digital currency that would act as medium of exchange between computers in peer to peer networks. It isn't a string of data as any other media file that could be simply transferred among many computers, since every transfer of cryptocurrency is recorded in the ledger called "Blockchain". Blockchain does act as one central record for all cryptocurrency transfer but there is no group of professionals responsible for updating this ledger. The updating task is done on decentralized basis i.e. anyone can take responsibility of updating the ledger with all new transactions and many really do to keep track of transfers; ensuring accuracy. Analogically, we can talk about a poker game with no poker coins at all and to continue the game people virtually bait their virtual money. To keep a track of losses and gains of every player, each player maintains his own written record of bets, hence keeping separately their owned ledgers. All ledgers at the end of the game would be brought together and compared, hence obtaining the correct record. Similarly, every single ledger owned will act as block of record which would indeed be a part of chain of blocks called "Blockchain". This decentralized logic gives rise to question about reduced security. Here, Cryptography comes into picture. Every account has a pair of keys (really, just pattern of data) which include a public key (people can use pass on coins to you) and a private key (you use to transfer coins to someone's account). Every transfer occurs after verification of sender's private key and additionally no key can be ever replicated. The sweat part here is, anyone keeps a ledger and updates it, must every time solve a hash function problem. For instance, bitcoin uses this hash function SHA256 only then can one update the ledger with one transaction. This painstaking solving procedure rings the question as to why anyone would bother to solve such a difficult problem just to update a ledger, well every cryptocurrency is supposed to have a built-in system to reward them automatically with 12.5 bitcoins. Ledger updaters are so also called Miners as they hit on chances to solve hash functions and earn this large chunk of earnings. Cryptocurrency is hence this intriguing topic that is both volatile and experimental. Investing in Cryptocurrency would be like investing to someone's project, success would earn you much and failure would leave you with lessons. Nevertheless, Cryptocurrency surely appreciates the fusion of imagination and Cryptography at its best, yet.



THE SATOSHI DICE

By Madhu Raut
(Senior Editor, IEEE VESIT)

Have you heard of the good old game called Pictionary? The pace with which we've been drifting towards technology, and celebrating what I like to call it, the Digital Revolution, we've earmarked ourselves for the utopian era. Coming back to our game, Pictionary- ask anyone to sketch their notion of money- you shouldn't be surprised to see the twentieth century wad of notes being replaced by a twenty-first century PC with a Bitcoin logo within it!

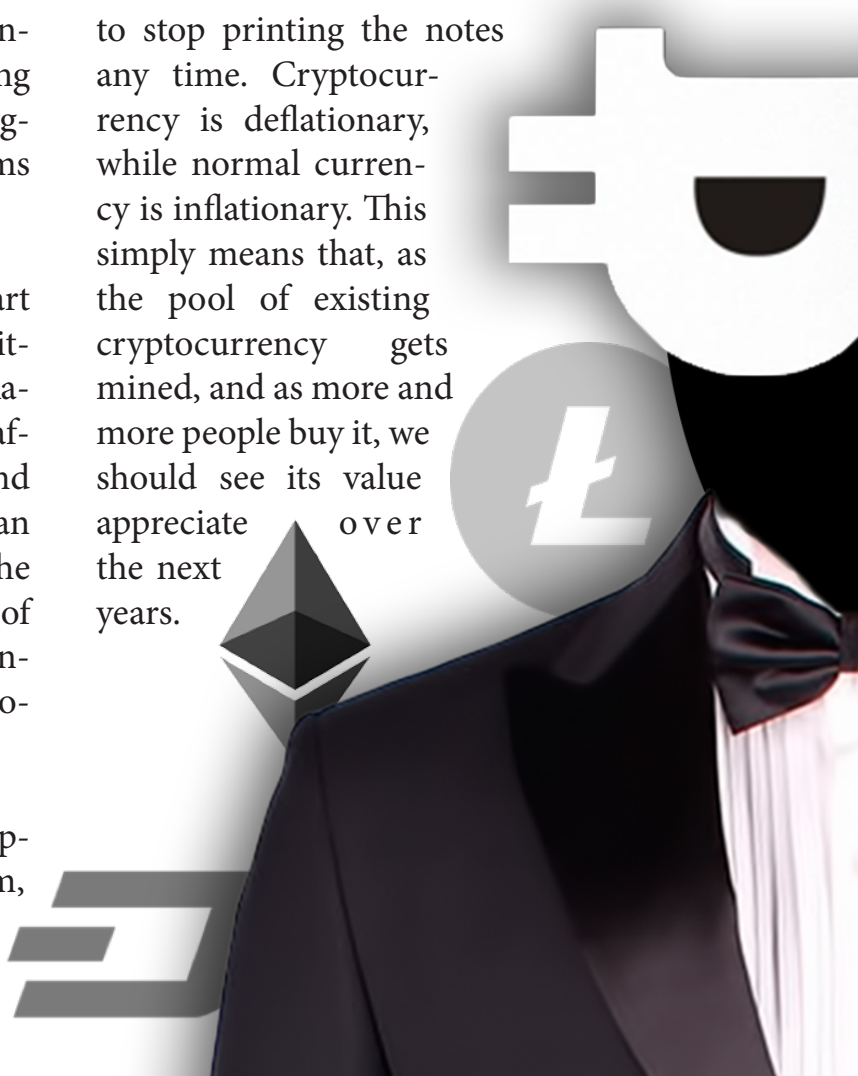
> *"People always overestimate what technology can do in two years, but underestimate what it can do in ten."*
>
> **-Charlie Cooper, Managing Director**
> (Blockchain Consulting Firm)

The Planet of Apes has forever been a believer of "change is the only constant". It's high time we gave ourselves a sanity check, connected to the WisdomFi (my version of a Wisdom WiFi) and updated our understanding of the current economy. "Cryptocurrency" is the word you'll stumble upon. Getting into the nuts and bolts of the single most significant invention of this century sure seems cumbersome, but is totally worth it.

If I were to give a hilarious kickstart to something so serious, I'd describe the Bitcoin to be the result of what Satoshi Nakamoto did with Technology and Finance, after watching Piko Taro smash his pen and pineapple (the PPAP reference provokes an uncanny Japanese resemblance between the two). This cover story provides a glimpse of where we might be when the government inevitably stops printing the faces of dead political leaders on expensive paper.

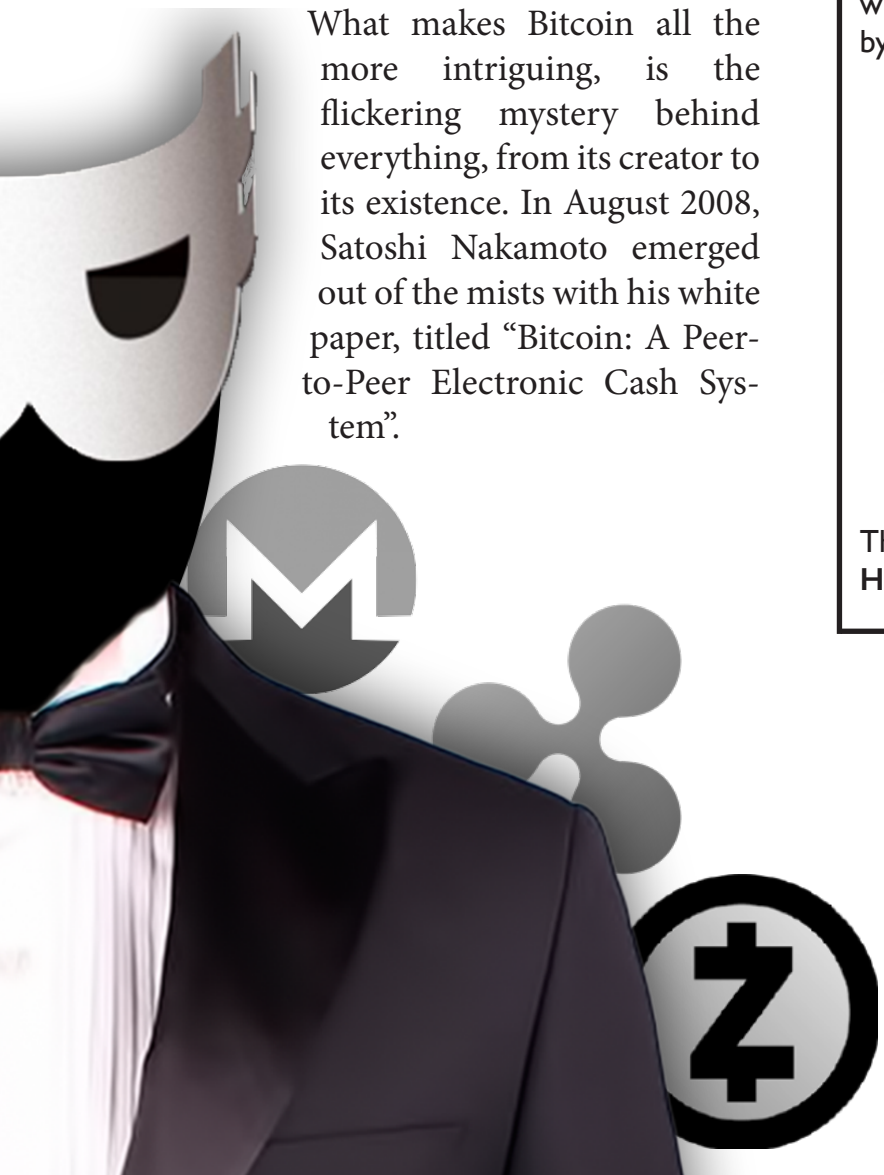
Cryptocurrency, short for "Cryptographic Currency", is a financial system, built on a global digital distributed ledger, called a blockchain. It is a decentralized system, meaning, that it isn't dominated by any central government or bank. Wearing suits, putting flags in front of buildings, makes people believe they're turning something immoral into moral. Likewise, the broomstick of freedom that cryptocurrency provides us, leaves the eventual consequences into our very own hands.

To understand why this system of economy is taking us by storm, we need to be aware of the shortcomings of the current economic system. In case of the normal currency, the central banks can decide to stop printing the notes any time. Cryptocurrency is deflationary, while normal currency is inflationary. This simply means that, as the pool of existing cryptocurrency gets mined, and as more and more people buy it, we should see its value appreciate over the next years.



Cryptocurrency will never experience inflation due to "printing". With the advent in technology, and the evil lurking in the dark, banks and governments are not very difficult to hack. Cryptocurrency, however, has come up with a fool-proof answer for thisissue, with what we call a blockchain.

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 currencies inspired by Bitcoin are collectively called altcoins and have tried to present themselves as modified or improved versions of Bitcoin. Some of these altcoins include: Litecoin(LTC), Ethereum(ETH), Zcash(ZEC), Dash, Ripple(XRP) and Monero(XMR).



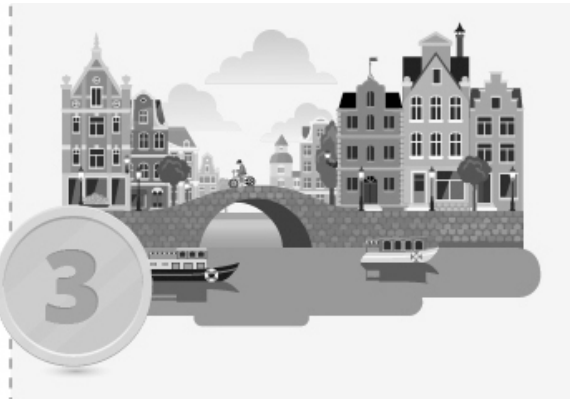
What makes Bitcoin all the more intriguing, is the flickering mystery behind everything, from its creator to its existence. In August 2008, Satoshi Nakamoto emerged out of the mists with his white paper, titled "Bitcoin: A Peer-to-Peer Electronic Cash System".

Floating buzzwords like "blockchain" hit us the moment we plunge into the sea of cryptocurrency, but the layman can barely visualise how it even looks. Understanding the mechanism of the blockchain and its benefits lies at the very core of this system. I was very impressed by Anders Brownworth's visual demo of the blockchain, and am about to explain the same.

FUN FACT!

Did You Know?

There are two streets in the netherlands ~ **Bierkade and Groenewegje** - that are known as **'Bitcoin Boulevard'**. Located alongside the Channel, a high majority of shopkeepers there will accept Bitcoin after an initiative submitted by **Hendrik Jan Hilbolling** and **Peter Klasen.**

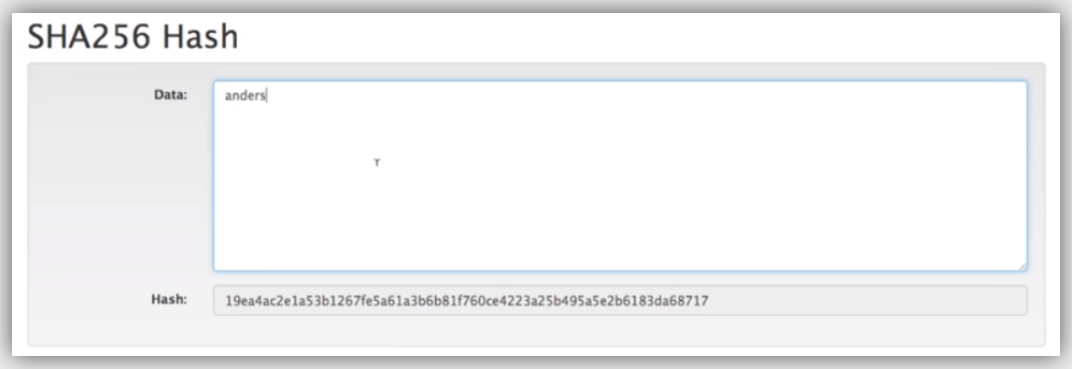


There is similar set up located in **Cleveland Heights, Ohio.**

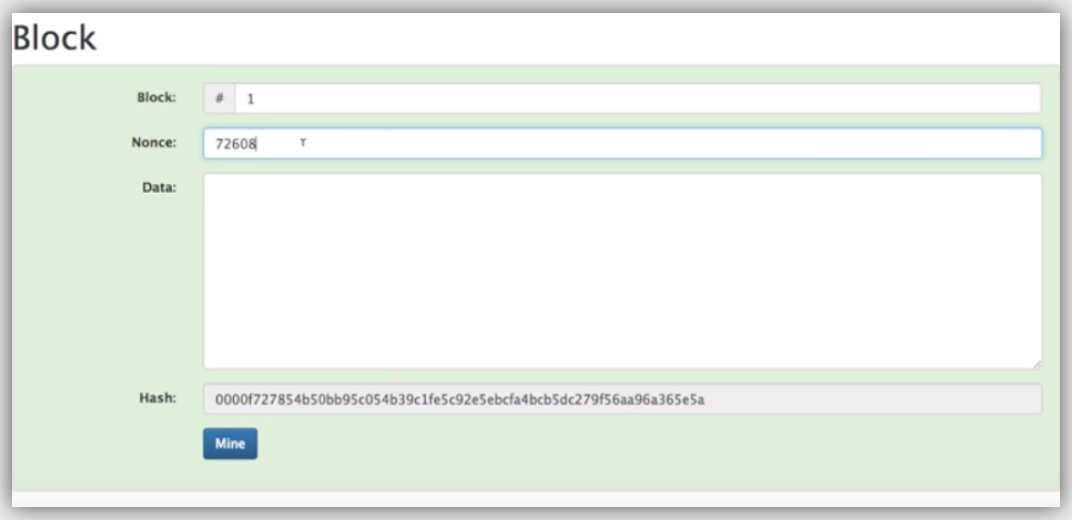
For More Information on Bitcoin:

Go to https://bitcoin.org/bitcoin.pdf
Or simply scan the QR Code:

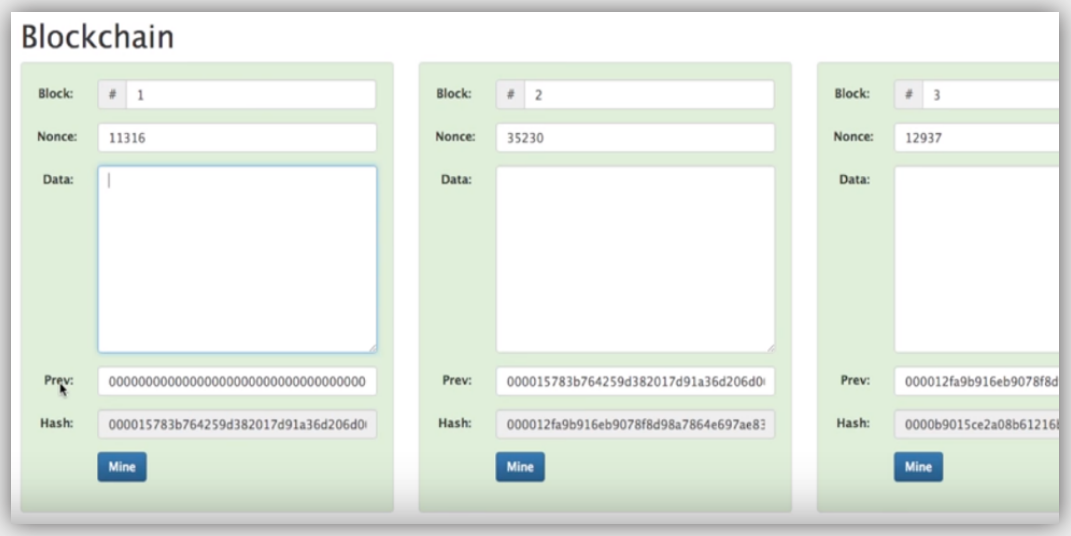
More than often, you'll encounter something called as a cryptographic hash function. The math involved in calculating it is just as scary as the name sounds, but for the sake of understanding the concept, we can assume a cryptographic hash to be just a bunch of random numbers. It's essentially a fingerprint associated with some digital data. Rest assured, if we run the algorithm for a given data, it generates exactly the same hash for it every time. As the name of the algorithm suggests, SHA256 generates a 256 bit hash always, regardless of the length of the data fed to it.



When we extend the idea of a hash into a block, two new parameters are introduced, Block# and Nonce. We assume the signed hash, i.e. a hash beginning with four 0s to be valid. Hashes starting with any other string of characters are considered to be invalid. When a hash becomes invalid, we need to adjust the nonce, to get the required signed hash(starting with four 0s). This, however, isn't the smart way of going about it, as you might spend hours or even days at stretch in front of your PC, but not figure it out. That's when the tiny "Mine" button comes to our rescue! It mines out the required nonce, and makes our block a valid one.

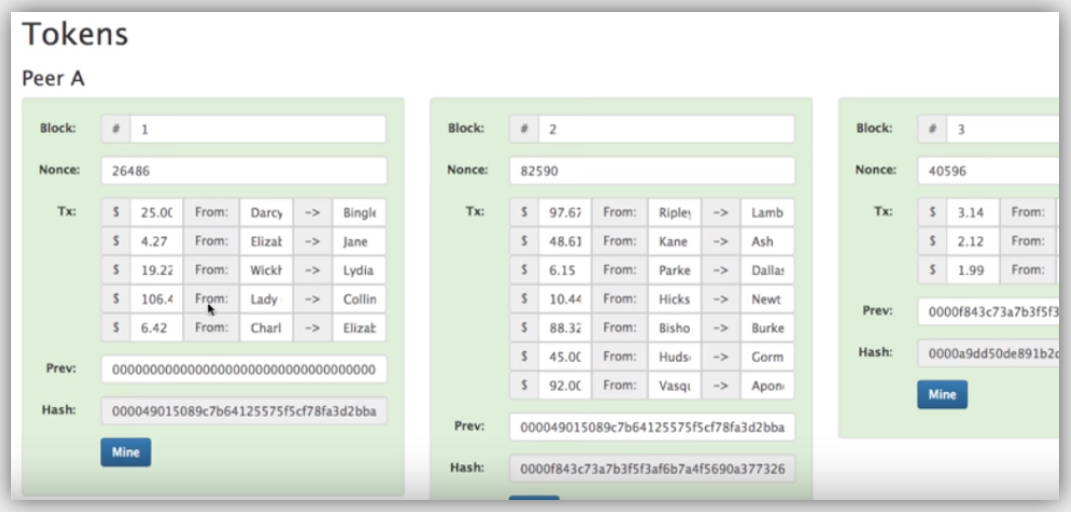


When we further scale up the blocks and integrate them, we finally get what we call the blockchain. Now, along with the previous fields, we notice an additional "previous" field, that determines the order in which the blocks exist on the blockchain. If any of the intermediate blocks is broken due to inconsistency of data, all of the further blocks also become invalid. This demonstrates a crucial feature of the blockchain, its ability to resist mutation.

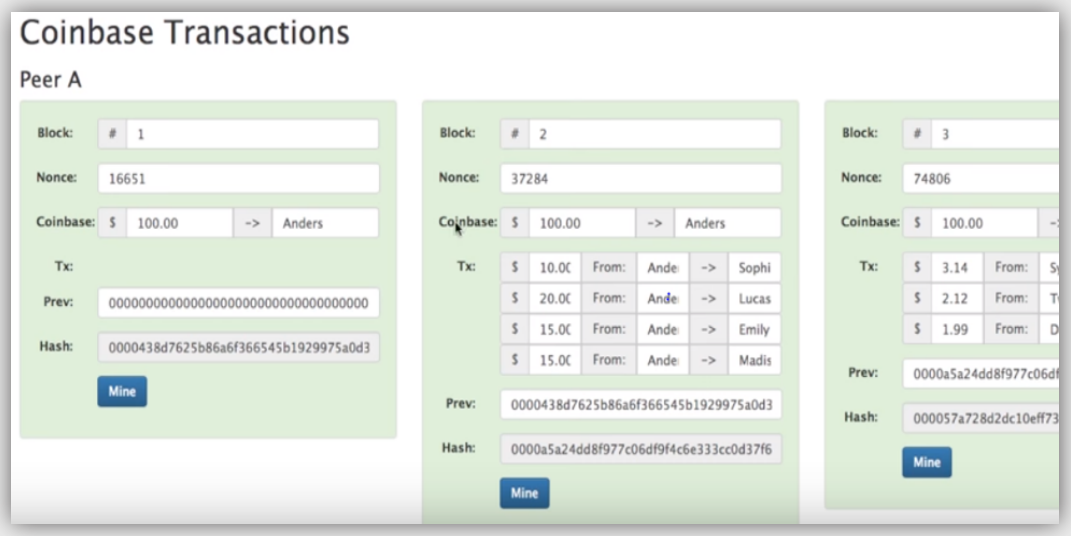


The Peer-to-Peer Electronic Cash System is formed by a number of peers(upto millions), existing on a distributed blockchain, each with a copy of the blockchain. In a decentralized network like this, with no central authority keeping a check on everyone, trust is pretty much a gamble. The distributed blockchain, however, creates a little democracy of its own. Let's say, we have peers A,B and C on the blockchain. If peer A turns out to have malicious intentions and makes changes in its blockchain; peers B and C still have the initial copies of their blockchain, that to not abide by the one maintained by A. In such a case, the majority's blockchain wins(B and C in this case), and all the other versions of the blockchain are dismissed.

All this while, we've been vaguely talking about data. When the concept of blockchain is run on top of a currency, we're referring to actual transactions, which constitute a token. Immutability is important to ensure consistency of all the transactions, on all the blockchains, of all the peers.

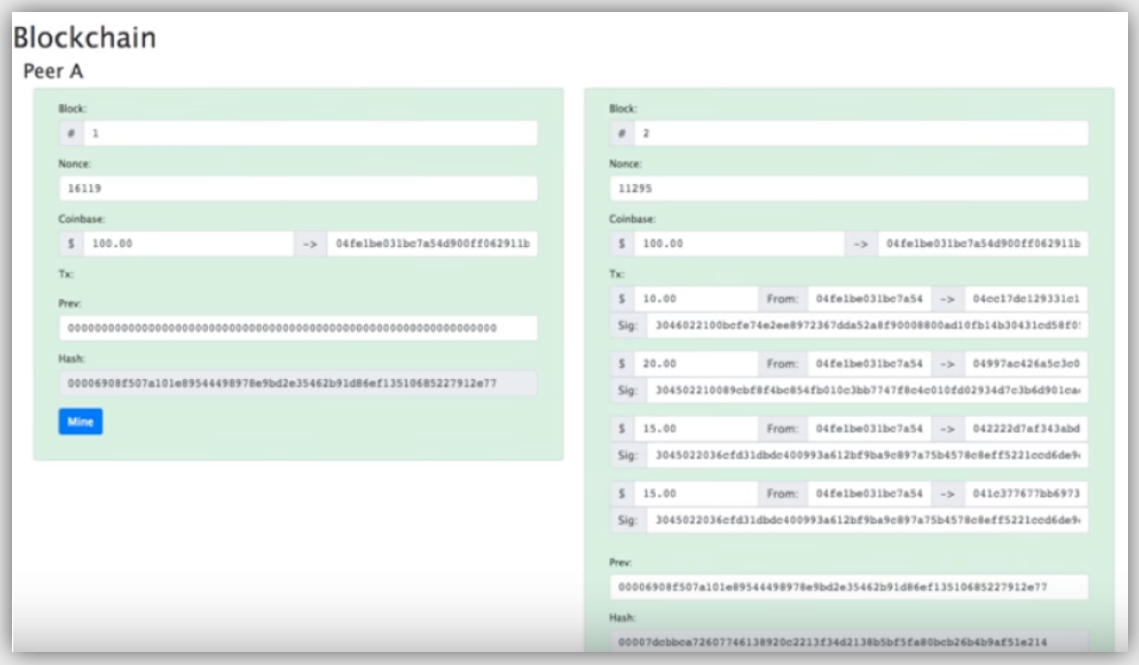


According to the principle of currency, dispersion needs to be controlled. The Coinbase Transactions essentially keep track of the balances in people's accounts. If Anders is giving Sophie $10, he needs to have a minimum balance of $10 before the transaction is successful.



ONE OBVIOUS QUESTION THAT MIGHT STRIKE YOUR MIND IS, HOW CAN WE STOP A PERSON FROM SPENDING SOMEONE ELSE'S MONEY ON THE BLOCK-CHAIN?

We come up with yet another cryptographic solution to this, message signature. For this, we need what are called as the public-private key pairs. There's a public key associated with each private key. As the names suggest, the private key is kept secret, whereas the public key is shared with all the other peers on the blockchain. The sender signs their transaction with their private key(known only to him/her), the message signature is generated and the receiver verifies the transaction with the sender's public key(known to everyone).
Double spending refers to the fact, that since in a cryptocurrency system, we're dealing with digital files, that can easily be replicated, both, the sender and the receiver can have copies of the file, and determining who the valid spender is, would be an impossible task. The message signature ensures that only the file signed by the valid sender is accepted.



Privacy is necessary for an open society in the electronic age.

By now, all the creepy terminology used by Satoshi in his white paper, might be making sense to you! I can bet on a hundred bitcoins, that the most hilarious, yet apt conclusion anyone could've drawn about the blockchain, is that of John Oliver on one of his Last Week Tonight episodes on Cryptocurrency:

"The blockchain is like a chicken nugget. Hacking the blockchain is like turning the chicken nugget back into the chicken."

-John Oliver

If you're FOMO(Fear Of Missing Out)-struck by that one guy around you who simply can't stop blabbering stuff about the Bitcoin, here's our favorite cryptography protagonist, Alice, amicably summarizing the steps involved in a Bitcoin transaction:

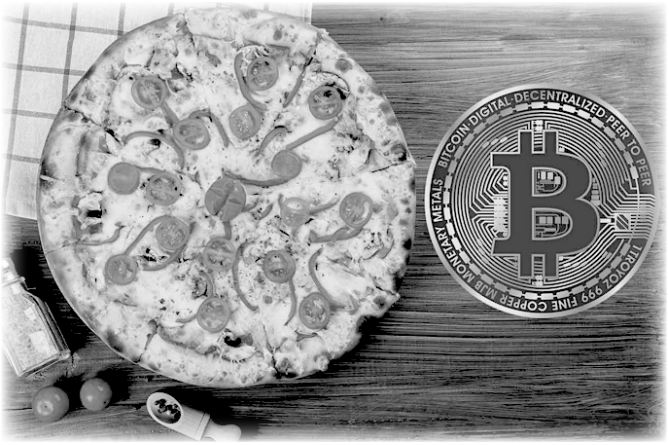
1. Alice initiates a transfer of Bitcoins from her account by signing off with her private key and broadcasting the transaction to other users.
2. The other users of the network make sure Alice's Bitcoin address has sufficient funds and then add Alice's transaction to a list of other recent transactions, known as a block.
3. Computers take part in a computational race to have their list of transactions, or block, added to the blockchain.
4. The computer that has its block added to the blockchain is also granted a bundle of new Bitcoins.
5. Computers on the network start compiling a new list of unconfirmed recent transactions, trying to win the next bundle of Bitcoins.

Nathaniel Popper's Digital Gold is a brilliant composition of all the intricacies in the works of the various Pied Pipers of Cryptocurrency. Ironically, the rats seemed to take a long time to get on this quest for the Holy Grail of universal money.

"Good money has generally been durable (imagine a dollar bill printed on tissue paper), portable (imagine a quarter that weighed twenty pounds), divisible (imagine if we had only hundred-dollar bills and no coins), uniform (imagine if all dollar bills looked different), and scarce (imagine dollar bills that could be copied by anyone). The essential quality of successful money, through time, was not who issued it- or even how portable or durable it was- but rather the number of people willing to use it."

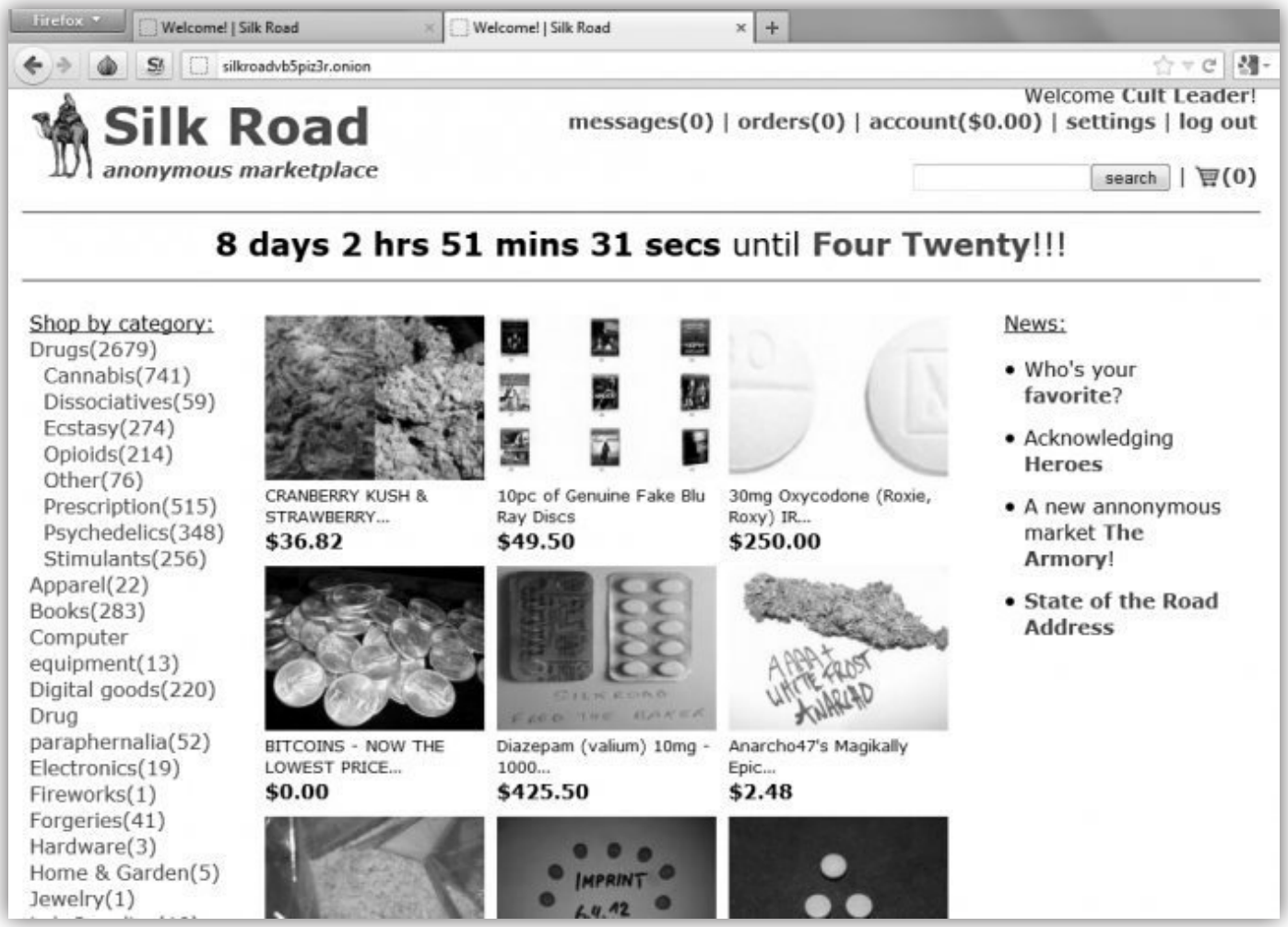
The Bitcoin code written by Satoshi was in C++(you can check out the codes for each of the versions on the Bitcoin Github Repository).

Laszlo Hanecz, a software architect from Florida, decided to test the vulnerability of this system. He understood that everyone on the network was trying to win the computational race with their CPUs; but the CPU was also running most of the computer's other basic systems, so it was not particularly efficient at computing hash functions. He quickly figured out how to route the mining process through his computer's GPU. Having stockpiled about 70000 Bitcoins by this time, he offered 10000 for a pizza. For the first few days, no one accepted them; but on May 22, 2010, a pizza guy accepted the offer and in no time, a delivery man knocked on the door of Laszlo's 4 BHK apartment, bringing two pizzas, fully loaded with toppings.



While pizza was one of the earliest "real" stuff bought using the Bitcoin, the range of products using this digital currency expanded in a dramatic way since an unassuming post on the Bitcoin forum:

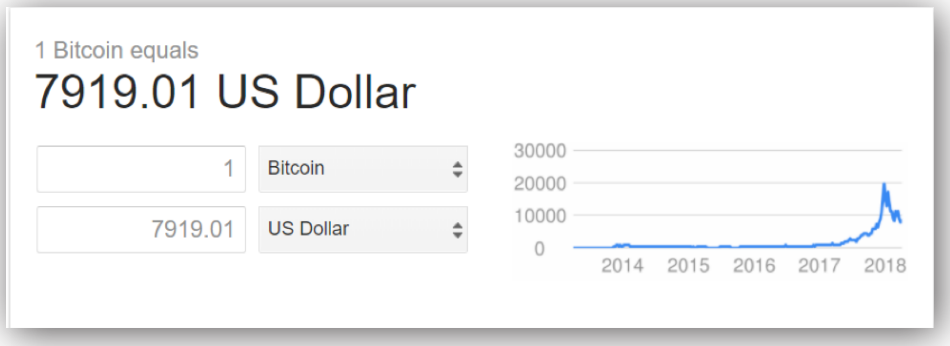
"Has anyone seen Silk Road yet? It's kind of like an anonymous amazon.com I don't think they have heroin on there, but they're selling other stuff."



The posting was made by someone with the screen name altoid. In real life, he was Ross Ulbricht. In building Silk Road, the drugs were the easy part; the harder part was finding a way to sell the drugs online, outside the watchful gaze of the authorities. For the years to come, Silk Road proved to play a crucial role in the infancy of Bitcoin, but has to be eventually shut down.

One of the most significant Bitcoin exchanges, was the one based in Tokyo, Japan; by the name of Mt. Gox. Launched in 2010, it flourished to be the world's leading Bitcoin exchange, handling upto 70% of all the Bitcoin transactions worldwide. In February 2014, Mt. Gox suspended trading, closed its website and exchange service, and filed for bankruptcy protection from creditors.

The most gigantic biz-magnet today, Bitcoin promises many more millionaires in our near future!



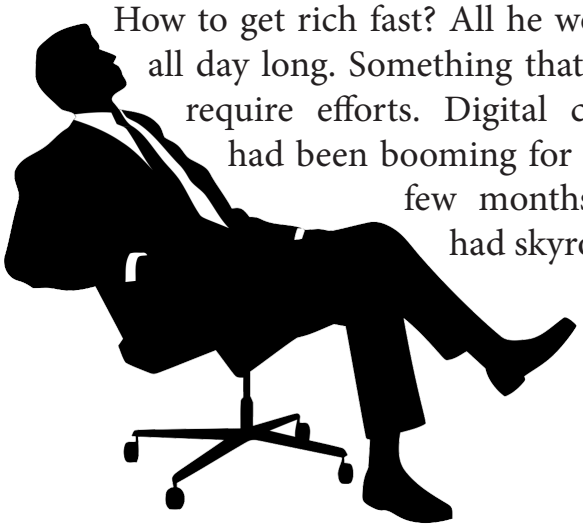
"Change from one kind of economy to another is likely to be painful, but when we get to the other side, it will be a lot better."

-Nathaniel Popper
Author of Digital Gold

VIRTUAL PRETENCE

By Rohit Kane
(Jr. Editor, IEEE VESIT)

Laid back on the chair, he looked at the ceiling. Life's been the same dull monotone for years straight. Like every habit needed a kick, all he wanted was a stimulus to grow out of the routine. His dreams touched the heavens, but his pockets complemented every single one of them. How to mint some? How to get rich fast? All he wondered all day long. Something that needn't require efforts. Digital currency had been booming for the past few months. Rates had skyrocketed.



He remembered, quite a while back he had made an account just for the sake of it. Curiosity made him login to the website again. However, now, something unusual greeted him on the front page. Normally the 7-8 zeroes followed by the decimal, had shifted to the left. Rather much shift was observed. He had a million bitcoins now. He was shocked, he refreshed the page on a spree, still the figure remained the same. He was beyond a trillionaire now. So much money, like the entire world rested on his fingertips! He didn't need a family anymore. Why would you need a company, when you've got wealth? Who would need loved ones, when you've got paper that runs this world? Who would want affection, when you can buy some? Now richest of the riches would bow down to him. His wishes would be their command.

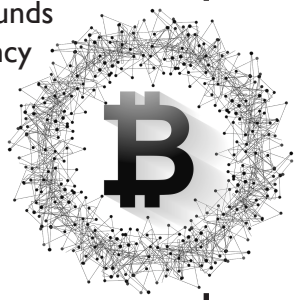
Lust was something he could only dream of till now, but a few virtual zeroes would now roll it in his arms, as he embraced pure poison. A bitter-sweet poison. Those who never heed him any attention, now would die for his mere friendship. A shout echoed across 2 cubicles. Boss was infuriated; piles of work pending, but a mind engrossed in dreams. Empty threats to fire him were now a routine. Who needed a job anyway? Now that money was on his side! Resignation letter ready with a signature, and a smirk on his face, he was all ready to slam them on his boss's face and walk off. He was secure! Not a dime to do with this company now. Building paradise on an invisible deck was quite risky, but his volatile mind was beyond comprehension. By now his wife had ringed him numerous times, only welcomed by his busy tone, as he cut her off after just a ring. The pretty lady next to his cubicle caught a keen glance at his desktop. Such a huge figure made her realize how much she'd been loving him all this while. Yet this fool blinded by miraculous luck believed it all. Drained the money like a river, clothes, fragrances, jewelry, all decked up against his credit.

FUN FACT!

Did You Know?

'Initial Coin Offering (ICO)'

An unregulated means by which funds are raised for a new cryptocurrency venture.
An Initial Coin Offering (ICO) is used by startups to bypass the rigorous and regulated capital raising process required by venture capitalists or banks.



Just as he planned to check on his new-found treasure, all he could see was a conversion; a conversion of the currency that marked his doom. All the money that he considered assets all this while was indeed a back-stab. As fortune slipped out of his hands, so did his high-flying interests, his 'new found love', his boundless dreams, most of all his ego. The virtual parameter that once made him roll in trillions had fallen like the steepest mountain, just like his imaginations had jumped from mount reality.

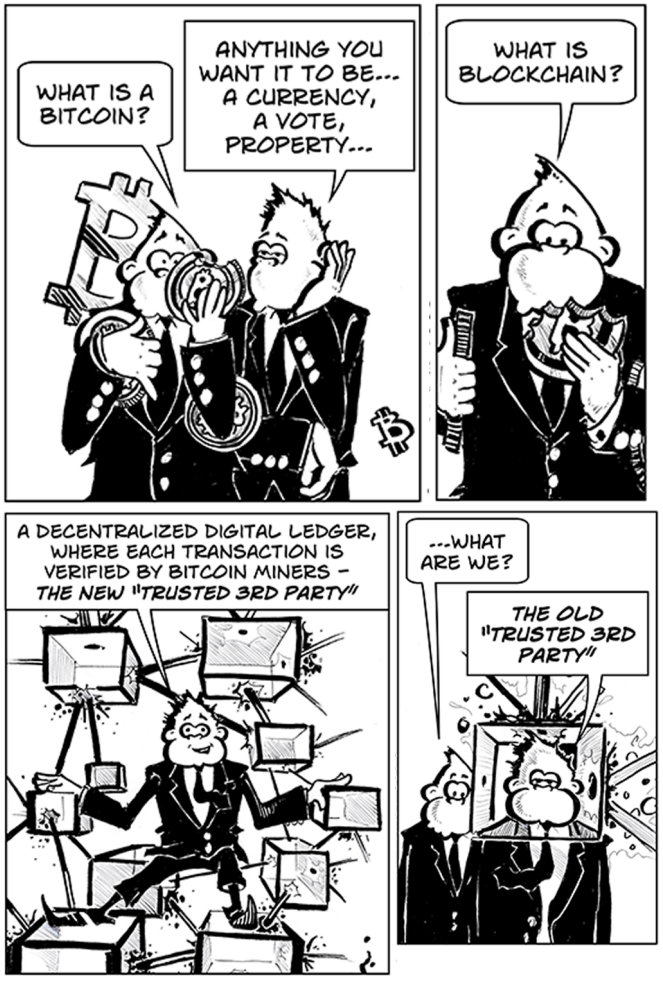
Suddenly with a loud bang, he felt a hit on his head; confused, still struggling to recover he got up from the ground. The chair seemed to have embraced the floor as well. What?! All this was just a dream, he startled. His mind playing games with him. Even though it was his subconscious, it had slapped him real hard, and back to the truth. Was money everything? Was lust everything? Was being an elite everything? He hadn't fathomed what family really meant, until now. What the eager eyes waiting for him at home really held for him! His dreams had taken him for a wild ride, a ride which taught him to accept the reality and stay grounded.

Virtual things do really boom, but their uncertainty is same as their fame. One day they're flying high. The next, they're crumpled up in pieces. He was done for the day, as he rubbed his face against his hands, and hovered his cursor over the shut-down.

Although late, he grounded safely.

Bitcoin is not "Unregulated"
It is regulated by algorithm,
instead of Governments,
Un-Corrupt.

- Andreas Antonopoulos



CRYPTOCURRENCY

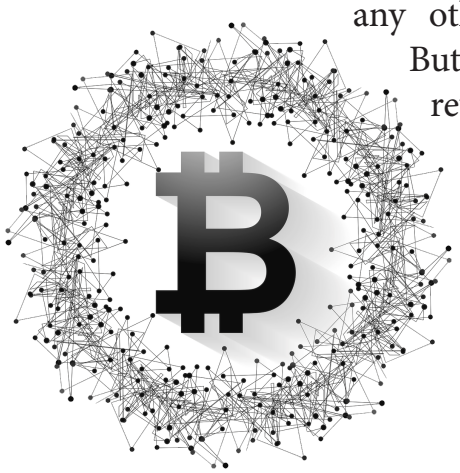
By Juyee Sabade
(SE First Prize)

For people who don't know what cryptocurrency is, to put it formally, it 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. 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. 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.

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

-Thomas Carper, US-Senator

If you take away all the complication around Cryptocurrency, it is just limited entries in a database system that no can change without fulfilling certain specified conditions. This may seem like the definition of any other bank system. But the mechanism revolving around the former, is significantly different. To put it in lay man's language, cryptocurrency uses a basic p2p technology where every peer has a record of the complete history of all transactions and thus of the balance of every account. To start with, someone requests a transaction, which is broadcasted to the p2p network which gives the transaction a validation using certain algorithms. Once verified, the transaction is added to a block of data, which is a database of transactions done by users. And then it is complete.



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. If 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. Cryptocurrencies are digital gold. Also, a fast and comfortable means of payment with a worldwide scope. While, they are used as mode of payments, they are also a fast-growing market for investors and speculators. The market caps of cryptocurrencies like Bitcoin, Ethereum, Ripple, Litecoin, etc. are in millions of dollars.

Questions & Answers!

1. Which of these is a kind of Crypto Currency?

a. Goldcoin b. Litecoin
c. Cashless d. Credit

2. Cryptocurrencies can also be referred to as?

a. Coded Money b. Credit Card
c. Virtual Currency d. Cash Policy

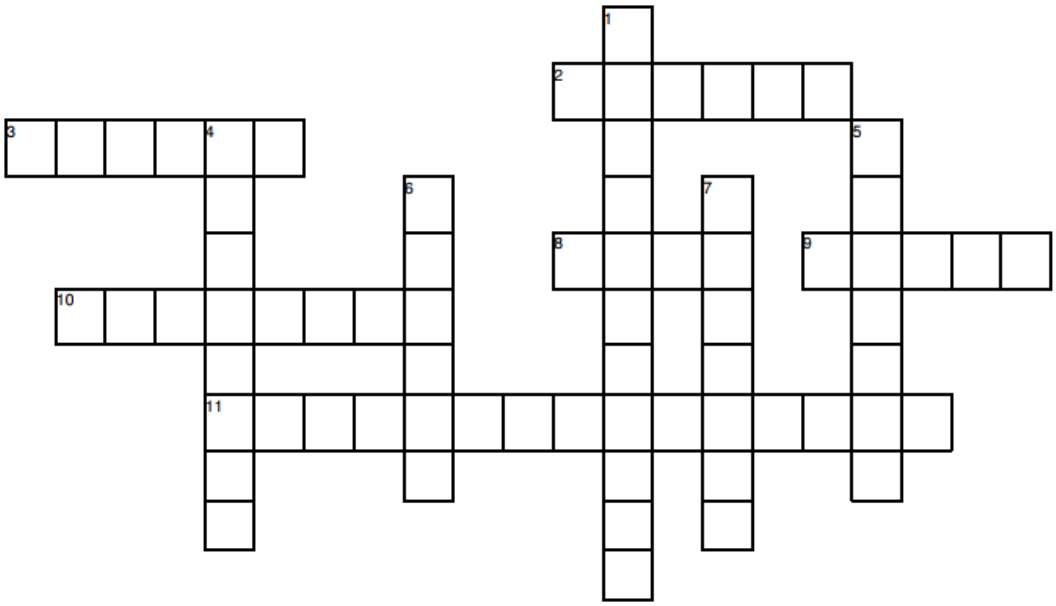
1-b, 2-c

Like any other business enterprise, Cryptocurrency comes with its own pros and cons. Looking on the bright side, Cryptocurrency has easy access, quick payments, costs less, private and highly secured. There are no third parties involved as it is a p2p system, no boundaries set and no chargebacks after the transaction is done. But, all the advantages do not mean there are no risks involved in dealing with cryptocurrency. There is uncertainty, a risk of robbery during payment, and there is no way to reverse the payment if one has changed their mind. Also, a lack of awareness and Knowledge makes it difficult to understand the transaction process and, it's not accepted widely.

As of now, Cryptocurrency has no major drawback and it's building its position in the market slowly. Every cryptocurrency comes with a promise, mostly a big story to turn the world around. Few survive the first months, and most are dumped by the speculators, when there is no hope seen in it. Both developed as well as developing countries are legalizing and regulating the use of cryptocurrency. Even countries with a high political restriction like Russia and China are trying to make it so people can be able to freely spend them.

Markets are dirty and ever-changing, but it can be concluded that cryptocurrencies are here to stay and change the world, and very soon we can witness the unbecoming of a revolution!

Cryptocurrency Crossword



Across

2. The supply of this old coin is still owned by the labs

3. the only relativly stable coin there is

8. Transactions often get tangled up with this one

9. This network probably brought you here

10. Digital silver

11. This one forked of from Dapps Dapps Dapps because Dapps Dapps Dapps forgot the D

Down

1. In the scripture of this coin the prophesy is foretold of a flippining

4. Dapps Dapps Dapps

5. The big one

6. Privacy Privacy and a bit of Privacy

7. It often calls upon a digital bull named Daedalus

THE BITCOIN MIRACLE

By Yash Marathe
(Coordinator, IEEE Vesit)

The Smith family had packed all their belongings. Their financial difficulties were growing day by day and they had to move to a smaller apartment way outside the city. Anthony Smith, the only earning person of the family just went through his entire childhood while packing things. He stood silently. His son, Howard asked, "Dad, why are you so quiet today?"; "Nothing son", he replied, "I never really thought that I'll have to leave this place."

Anthony's childhood friend, John who was helping them in moving, came to the apartment. "So, all packed up?", John said, "But before we leave, let's have a last pizza.", "By the way, Anthony do you remember that way back in 2011, we used to mine Bitcoins?", John asked. "Yeah, what about that?", Anthony replied. "The trending news around the world is that Bitcoin's price is growing exponentially day by day", John said. "Wait, what is bitcoin?", Howard asked. "It is a cryptocurrency. Let me explain this to you in a straightforward way.

In 2010, 10,000 bitcoins would get you 2 pizzas. Now 1 bitcoin is worth about 20 million pizzas", John said. Anthony just realized that he could solve all the problems of his life with a few bitcoins. They had stored the bitcoins in a hard disk in 2011 when they used to mine bitcoins without realizing its potential. He left the pizza and ran as fast as he could to the find the hard disk. He opened almost everything that they had packed over the month; but he couldn't find it. It was like the last hope of getting his life back on track was about to get lost. "Howard", he yelled, "Where is that bag with all hard disks and old laptops?" That scream made Howard worry a little. "Didn't you ask me to trash it? I threw it in garbage today", Howard said. "Of course, I did", Anthony sighed. He stood there with disappointment and realized that that there was nothing he could do to change his life back to financial stability.

Anthony's wife Sarah heard all the noise and came to the hall. She asked, "What is happening over here?" Anthony wasn't in the state of explaining so John stood up and said, "Back in 2011, we successfully mined bitcoin blocks and then we stored the bitcoins in a hard disk because at the time they were worth only $0.31 per bitcoin. It turns out now they are worth $2856 per bitcoin but Anthony realized that he just trashed that hard disk in the garbage and there is nothing we can do to get them back." Sarah remained quiet and arranged the thoughts for a moment. It's amazing how women don't panic at demanding situations when men have lost all their hope. "Wait, we can go to the garbage disposal and find it there", Sarah suggested.

"It would take months to search our hard disk. There are tons of garbage from all over the city over there." "Don't they separate the solid waste and all the electrical equipment?"

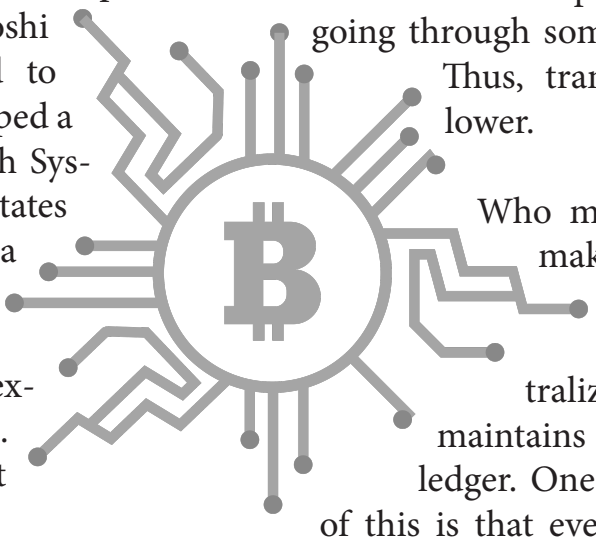
The Smiths had gone through a lot of trouble over the last the few weeks and it looked like the troubles were finally going to end. Although there was a small hope of getting back their old life, but the Smiths decided to fight for it. They managed to get to the garbage disposal and through John's help, they got in the solid waste disposal. It wasn't going to be easy. Though, they managed to separate the waste, but still there was a mountain of hundreds of kilos of electrical equipment lying in front of them. Anthony and John kept searching. A thousand thoughts went through Anthony's mind. He didn't expect much. He just wanted to give his family back the life they deserved. However, after hours of searching, they couldn't find it. They returned home.

While returning home, Anthony realized that he had stored a few bitcoins in John's hard disk. "Wait, remember that day, when my hard disk had some issues so after mining the bitcoins, we stored them in your hard disk?", Anthony asked. "Wow, yeah! But I think there are very few bitcoins in my hard disk", John replied. "A few bitcoins have a lot of potential to change my life right now", Anthony said. They drove to John's place and to their surprise John's hard disk had bitcoins of worth around $15,000. They both smiled at each other and John said, "So, Anthony, looks like that wasn't the last pizza we had at your apartment!" After weeks, Anthony was smiling and was happy. Deep down his heart, he realized that no matter how tough life gets, miracles do happen.

CRYPTOCURRENCY

By Dhaval Bagal, D7B
(SE Second Prize)

What is Cryptocurrency? A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. Didn't get it? Let us understand it in a simpler manner. Before beginning with the most curious question - What is Cryptocurrency? let us first understand it's origin. Cryptocurrency emerged as the side product of another invention. Satoshi Nakamoto, never intended to invent BITCOIN. He developed a peer to peer Electronic Cash System. A simple definition states that they are just entries in a database which no one can change without fulfilling specific conditions. Take an example of your bank account. The balance in your account is just an entry.



It can be changed only when you get the physical coins and notes (i.e. a specific condition is satisfied). Thus, money is all about a verified entry in some kind of database. How it works? Several currency exchanges exist, where you can buy and sell bitcoins for dollars, euros and more. Your bitcoins are kept in your digital wallet on your computer or mobile device. The bitcoin network is secured by individuals called miners. Miners are awarded new bitcoins for verifying transactions. After transactions are verified, they are recorded in a transparent public ledger and the transaction is done!

Miners are the people who mine for bitcoins. They are responsible for verifying transactions. Ledger at a basic level is a file that contains names and balances of the individuals. Signatures are analogous to signatures on cheques. When we want to send some amount to someone, then the transaction message (containing account numbers of sender, receiver and amount) along with the private key (analogous to password) of the sender is fed into a special cryptographic function and the output is a signature. These signatures are unique to each transaction. Cryptocurrency system is decentralized system, meaning there is not central authority to control everything. Cryptocurrencies are transferred from person to person without going through some third party like bank. Thus, transaction fees are much lower.

Who maintains the ledger and makes sure no one cheats? Since the cryptocurrency system is decentralized, so every participant maintains their own copy of the ledger. One surprising consequence of this is that everyone can see everyone else's balances, however the identity remains hidden, since account numbers are used instead of names. Hence there is some level of anonymity.

One question that arises is, if everyone maintains their own ledger, then how is synchronization achieved? The idea is simple, when you want to send a money, you broadcast a transaction message to everyone containing your account number, the receivers and the amount. The transaction message along with the private key of the sender is fed into a special cryptographic function resulting in a signature. The miners verify these signatures to ensure that the money has come from the real owner. After the verification all public ledgers are updated.

THE TRUEST CURRENCY

By Hitesh Jetwani
(SE Coordinator, IEEE VESIT)

Welcome to my world, it's as you'd call, "The Future". The year is 2051, we've asked for far more than the previous generation could ever imagine. All the base knowledge of life and math are included within babies the moment they are born, thus a finger painting toddler can integrate complex functions with ease and when they grow up they are genetically engineered to stop aging on their 27th birthday. Some other features of this life are, a secondary Mars colony, a trans-continental loop system which connects what is left of humanity, a constant heads up display built right in everyone's eyes which connects to the pal assistant who is also everyone's best friend, and almost all banking systems have been abolished, thanks to the unified currency -£loins and the single ledger associated with it.

We are all but killing time,
until time kills us

- Unknown

The amount of which they have is constantly displayed in unmissable green screeching through the blue text on the HUD. Everyone gets 1 coin on their 27th birthday; but unlike every utopian trait of this future, the devil is in the detail; well if the details were written in an alarming red and caused 90% of the deaths, as when the account reaches zero, that person "Times Out", or dies... Am I forgetting something...? Everyone is charged per heart beat! This fee has to be paid to our president business; president Musk takes care of all basic life essentials. This story looks closely on two specific "time zones" and this is the story of me- a glitch in this system. So the stage is divided in 2 zones, the first being what used to be Bangalore- a poor manufacturing area where people generally have coins worth 24 hours or less on their clock at any given time; and Mumbai- the wealthiest time zone, where people have enough time on their clock to essentially be immortal, also the home city of president. I used to be a miner, running and coding for what's left of the few unmined coins, but would not fetch much from the pool I contributed towards just a few M hashes per day enough for me and my 50-year-old mother.

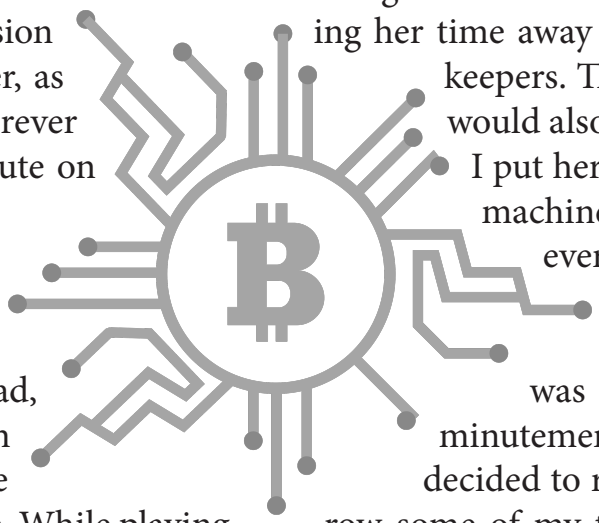
This life of rhythm, logic and predictibility, well, it got out of my hand when I rescued a drunken man from an attempted robbery by a gang of "Minutemen" (time-robbing thugs).

The Sage (as I call him now) revealed that the people of Mumbai hoard most of the time for themselves to live forever, while constantly increasing cost of living keeps the working class on taps as most of the coins are mined, not to mention they rewrote the central ledger a few years prior so that the family could have an almost inexhaustible amount of coins.

One faithful morning, the Sage transfed 116 years of his time to me, before timing out and falling off a bridge. I decided to infiltrate the streets of the presidential town but before that I had a debt to repay, one of friendship to my blood brother, Reed. I revealed what just happened. Reed warned me, that having so much time within Bangalore will get him killed. Bidding adieu to the fellow, I handed him ten years in return for their years of friendship. I went back home with a sense of achievement, only surpassed the first time I made a rig, but my mom was nowhere to be found, so I checked the ledger only to find she was timed out and I took the second worst decision of my life of not reviving her, as she would have hated me forever if I'd have spent even a minute on her, leave alone a century.

The following morning, I left for the city. Going old fashioned, I took the road, visited a local casino and ran into a rich fellow from the city and his daughter, Valerie. While playing poker, bankruptcy was just a chip away, but forcing the trader to fold, I won more than a millennium in a flawless gamble. Impressed, the lady invited me to a party at her mansion. Buying a new Koenisegg, I rode to the party. After a quick dance, down at their private beach, I tempted her into a moonlit dip in the waves; which I didn't know would be her first brush with danger, outside the controlling grip of her father. She received a notification from her home, reading which she was shocked and insisted on going back inside immediately. I did feel something suspicious was going on, judging her sudden stammering, but I shrugged it off to cold breeze. Once back indoors, I had the shock of my life; being greated by a couple of Ledger keepers (also known as timekeepers or policepeople). They had a warrant against me that accused me of theft and murder.

I denied, but as I was a case almost certain to be a glitch, and no glitches are allowed, they extracted almost all my pleas, the keeper confiscated all but 2 coins- worth 2 hours of life. I asked him why he's investigating a suicide. He started explaining that the higher ups don't like glitches because that allow people from lower classes to move up the food chain and that's the position they want to keep to themselves as long as possible. Left with little choice, I took the girl as a hostage and drove her hand in a curl, stealing her time away in front of the shocked keepers. They wouldn't shoot, as it would also kill the pretty little girl. I put her down in my new speed machine and drove away. However, being me is difficult, bad luck finds a way of catching up with me. I was ambushed by a gang of minutemen. Reversing my steps, I decided to run back home and borrow some of my time back from Reed. I was greeted by his wife, Sue, who informed me that the last person I could have turned to, drunk his self to death with 9 years on his clock. Blaming myself for the stupidity, I left.



FUN FACT!

Did You Know?

The furthest place you can reach using **Bitcoin**, is **space**.

Virgin Galactic are accepting **Bitcoin Payments** as a way of **getting to space in their journeys**.

Valerie pawned her diamond earrings for extra time, and I decided to move ahead with my plan, calling up her dad to ask my 1,000 year ransom. When payment was refused, I decided to release her anyway. Before leaving, she confessed her love to me and told me a girl was coming in the chain and graced me 1000 years. Banking on her, I bet on the worst possible terms and won over a million years, now I could move to the city and start anew or die a hero, I decided to give away my money to the community I grew up in and release them from the shackles of slavery. Giving everyone enough time to try for something epic and releasing them from the mundane, atleast temporarily! Is there really a way to fight against the machine, especially when the family owns the base ledger? I got together a band of friends- the smartest I know of. With the confidential information that we had, we found a divident fork coming up on 28th June on the Presidential Day. So, we decided to do the unthinkable, get away from the system between; we decided to give away our immoratility so that we can live, and not just survive! We started with a simple jail break of our HUDs, next was a complex surgery, and giving up on the boring details, we now can't access any technology nor purchase anything, so we live off in the forests and wait for nature to claim us.

Someone's just solved a three-year-old £40,000 Bitcoin puzzle

It took three years, and a massive inflation in Bitcoin's value, for someone to solve this puzzle painting

Someone has just become very rich after playing a wonderful game of Where's Wally (or Where's Waldo) with a piece of artwork hiding 4.87 Bitcoin.

The painting was first put on Twitter in April 2015 and the winner was found yesterday when the money was quietly removed from the hidden Bitcoin wallet.

The puzzle didn't actually contain 4.87 physical bitcoins but instead hid a hash number to an associated wallet. At the time of the artwork being created, a single bitcoin cost $240.57, making 4.87 bitcoin equated to around $1,170 – or £780. In 2015, that's still a very generous prize pot for a puzzle painting. Now though, that same 4.87 bitcoin is worth a staggering $50,000, or £35,170.