TECHZONE

WWW.WOXSEN.EDU.IN

WU™

WOXSEN
UNIVERSITY
SCHOOL OF TECHNOLOGY

THE SCIENCE OF TODAY IS THE TECHNOLOGY OF TOMORROW

-Edward Teller
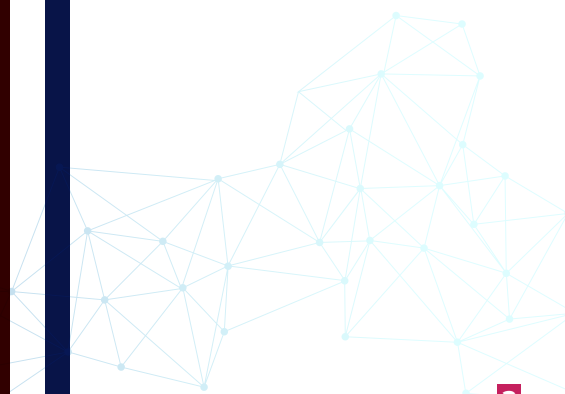
1

CONTENTS

ADITHYAHAVALDAR,
EDITOR-IN-CHIEF

VAIGARAISATHI,
EDITOR

VARUNTEJA,
EDITOR

POLYMORPHIC CODE AND VIRUS

by Srikumar K S

We all know that computers are prone to be corrupted by viruses. A computer virus is a piece of code written in such a way that it spreads from one computer to another and corrupts it.

In the era of TechnologyTechnology, these viruses pose a significant threat to people's privacy, and to detect these viruses, we have antivirus software that protects our system from getting compromised. In this article, we will see about one such virus that can hide from the antivirus software.

Polymorphism

Polymorphism refers to the proficiency of an object to change itself into different forms. When we apply this phenomenon to coding, something called a polymorphic code is formed. This code can mutate its base code while keeping the main algorithm intact that is, the written code changes itself every time it is run, all while still completing the task given to it. For Example, 10 x 2 and 4 x 5 both provide the same answer, but it does so using different values.

Polymorphic virus

A computer virus is known as a polymorphic virus when it uses polymorphic code, and to the question of why it uses it, it is to conceal itself from antivirus software. Most of the software out there made to find and erase viruses try to locate the virus by scanning each folder and data packets in the system, and if the software finds any piece of code or patterns of known viruses, it will take necessary steps to erase it, but in the case of a polymorphic virus it is hard to find it as it keeps changing its code or "mutates."

"1260" was the first polymorphic virus that Mark Washburn wrote in 1990. The hacker Dark Avenger wrote a better polymorphic virus in 1992 to prevent antivirus software from recognizing it.

Some well-known and dangerous polymorphic viruses exist URSNIF, AIRLOCK, VOBFUS, and BAGLE or UPolyX.

How Does it work

This is a widespread problem; The most popular or sought-out way to hide a code is encryption. First, the main body or 'Payload' of the code is encrypted, which will appear like gibberish. Then, a function is used to encrypt and decrypt the code, and the main code is decoded and then executed. Still, just this doesn't make a code polymorphic. The ability to mutate or generate a new encryption/decryption function with the constantly changing code is what makes a code polymorphic. The virus relies on special mutation engines to change the decryption process every time the virus infects the system.

What Happens

As a polymorphic virus can appear in any form, be it malware or trojan, so one needs to pay close attention to what the system displays. The flowing may happen if your system is affected.
•The system may issue strange requests like "enter a password" or sensitive information.
•The computer suddenly slows down and heats up.
•The system may not give you access to the files you need
•A web browser may suddenly take you to an unnecessary website, or a pop-up ad occupies the screen on a website that doesn't usually use these types of ads.

How to get rid of and prevent being affected

If the computer has a system image before it was affected, we can factory reset it to remove the virus, but one must be very sure that the virus did not affect the restore point. Unfortunately, if you are not sure, the only way is to reinstall the OS (Operating system). That is the main reason this virus is dangerous, as there is no particular way to neutralize it right now, and although studies are being done, they are not definitive.

Preventive Measures (for any virus)

•Always keep your system and the antivirus software up-to-date
•Never click on suspicious links or download unwanted attachments
•Back up the data regularly so that when a virus attacks, you can reset the system
•If you think your system is hacked, constantly disconnects from the internet and go to cyber security

Comment

As far as computer viruses go, all of them are very dangerous. However, it is better to be safe than to lose all your data, so I think one should be very precautious while browsing the web. Though these kinds of polymorphic viruses are dangerous, thorough research and study are being done. Through AI and Machine learning, it can be possible to neutralize a polymorphic virus, which tells how much the technology is advancing. Therefore, it is only appropriate for us to keep ourselves up-to-date to not become prey to invaders or viruses.

LEARNING THE HUMAN LANGUAGE
by Sathi Vaigrai

Speech processing is the subject of speech signals and the refining methods of signals. These signals are refined in a digital illustration so that speech processing can be deemed as a special event of digital signal processing, implemented to speech signals. Speech processing features comprise the retrieval, administration, accommodation, assignment, and product of speech signals. The information is designated as speech identification, and the product is designated as speech synthesis.
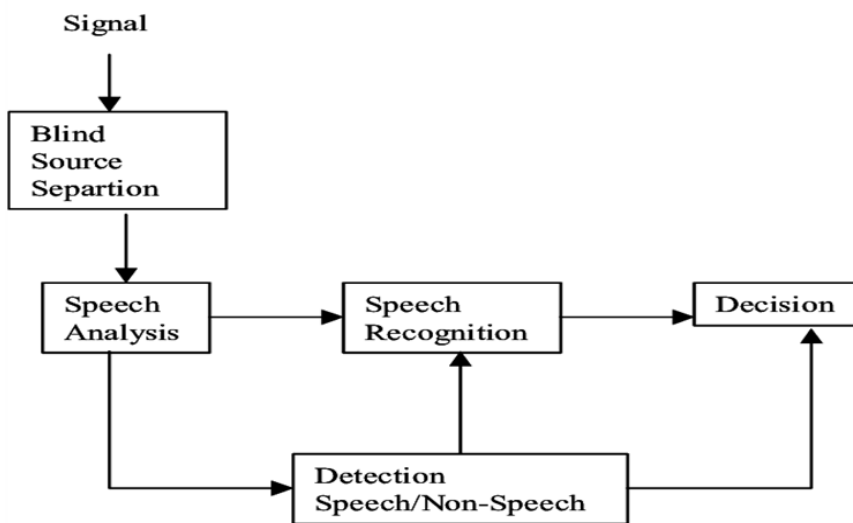

Initial efforts at speech processing and identification were principally concentrated on learning a few uncomplicated phonetic components such as vowels. Near the primal 2000s, the authoritative speech processing tactics began to move beyond Hidden Markov Models in the direction of increased modernistic neural interfaces, including deep learning. There are multiple procedures of speech processing: Dynamic Time Warping, Hidden Markov Models, Artificial neural networks, and Phase-aware processing.

Dynamic time warping, abbreviated as DTW, is a design for estimating correlation within two transient progressions, which might diversify in movement. Customarily, DTW is simply a process that determines an appropriate union between any two given classifications with specific constraints and rules. Hidden Markov Model (HMM) is a mathematical Markov model in which the arrangement is registered and considered to be a Markov means with unobservable ("hidden") events. An artificial neural network abbreviated as ANN is established on a compilation of united units or nodes designated as artificial neurons, which roughly represent the neurons present in an organic brain. Like the synapses that occur in an organic brain, every link can transfer a sign from an individual simulated neuron to a different neuron. Phase-aware processing is customarily reckoned to mean a stochastic homogenous variable and, therefore, worthless. The wrapping of the phase is the leading cause of this occurrence.

Speech processing is the subject of speech signals and the refining methods of signals. These signals are refined in a digital illustration so that speech processing can be deemed as a special event of digital signal processing, implemented to speech signals. Speech processing features comprise the retrieval, administration, accommodation, assignment, and product of speech signals. The information is designated as speech identification, and the product is designated as speech synthesis.

Speech processing enables capable machines, such as smartphones, to socialize with users by verbal expression. Siri, Apple's voice-recognition service, is an example of this. This study of speech studies and its variants could be critical in a world where the technological connection between humans and machines is increased. Further improvement in the analysis methods is expected, and with improved data at our disposal, human-machine interaction will only get better as time progresses.
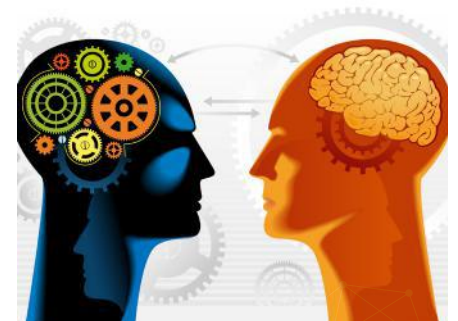
Exploring BlockChain Technology

by Bindu Hasitha

DLT (Distributed or shared Ledger) - Digital system for recording the transactions of an asset wherein transactions are recorded in multiple places at the identical time.
Decentralization is achieved through consensus, a fault-tolerant mechanism used to reach the necessary accord on one sole state of the network.

Blockchain is a kind of DLT that records and disseminates the transaction details of any digital asset across the network of Nodes (Computer systems).
Each Block contains or is structured in the following way:
1. Blocks store data regarding transactions; as an example in Bitcoin Blockchain, a block stores data like From(Sender), To(Receiver), and the quantity of your most up-to-date purchase.
2. Blocks store data regarding who is participating in transactions rather than revealing your actual name. Your purchase or asset details are recorded employing a unique "digital signature" without identifying information.
   3. Every chunk contains a unique code known as a "hash" that differentiates it from the others.
      * There are three primary types of Blockchain:
                  1. Public Blockchains like Bitcoin and Ethereum
                  2. Private Blockchains like Hyperledger and R3 Corda
                  3. Hybrid Blockchain like Dragon chain

Public BlockChain (Bitcoin and Ethereum):

A public blockchain is a permissionless blockchain. Public Blockchain permits anyone to participate as users, miners, developers, or community members. Every transaction on public blockchains is crystal clear, which implies that anyone can view/read the transaction details.
1. Public blockchains are fully decentralized, with no entity controlling what transactions are recorded or the order in which they are processed in the Blockchain.
2. Public blockchains are often extremely censorship-resistant since anyone can join the network, making it arduous for authorities to shut them down.
3. Public blockchains have a unique cryptocurrency to incentivize all the nodes(computers) within the network.
4. Examples - Bitcoin and Ethereum

Problem Statement:
All pharmaceutical businesses are concerned about the spread of counterfeit pharmaceuticals. Therefore, there is a need to create a practical solution to incorporate track and trace products in the supply chain to identify spurious medications that are purposefully or fraudulently mislabelled in terms of identity/source.

Solution:
The solution is to provide a single integrated platform for different entities like Manufacturers, Transporter, and customers to enter and retrieve the details of the product through a DAPP (Decentralized Application). It consists of varying User Interfaces' for entering the product details at each stage (like manufacturing, transporting, and customer) stored on Blockchain, automating the tracking process using intelligent contracts (Fuel to the DAPP). The process that happens on the Blockchain is purely Backend that the user doesn't have access to. Therefore, developing this solution will give access to product information both to the Intuitive persons out there and knowledgeable persons securely and reliably (Use of Blockchain), making the customers assured about the product and eventually helping to reduce the number of people affected by tampered medicine products.
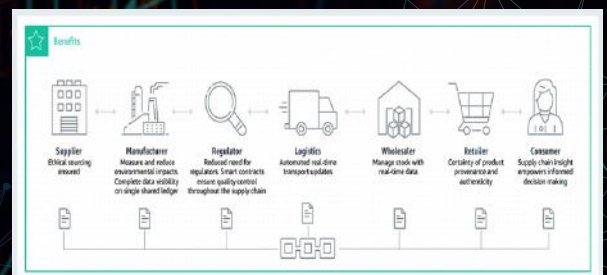
HONEYPOT AND HOW IT LURES CYBER ATTACKERS

by Sabahat Shaik

A honeypot is a computer security mechanism that identifies, blocks or mitigates unapproved access to information systems. A honeypot is typically made up of data that appears to be a genuine part of the site and contains valuable information or resources for attackers. However, it really is isolated, supervised, and capable of preventing or analyzing attackers.

Large corporations and cybersecurity organizations often use honeypots. It assists cybersecurity researchers in learning about the various attacks used by attackers. However, it is suspected that cybercriminals also use honeypots to deceive researchers and spread false information. A honeypot is typically expensive because it necessitates expert skills and resources to enforce a system to ensure that it appears to provide a company's assets while still blocking backend attacks and access to any manufacturing systems. Honeypots are categorized based on their deployment and the intruder's involvement.

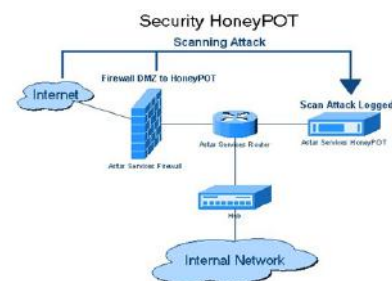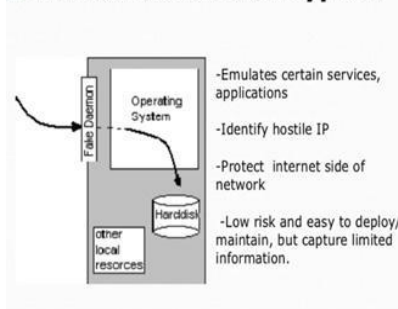Honeypots are divided into two categories based on how they are deployed:

•Production honeypots are convenient for using, collect very little data and are mainly used by corporate entities. An organization places production honeypots inside the production network alongside other production servers to improve overall security. Production honeypots are, typically, low-interaction honeypots that are more easily deployed. They offer less information about the attacks or the intruders than research honeypots.

•Researchers use research honeypots to analyze hacker attacks and deploy various methods to avoid them. Honeypots are used to gather data on the true motives and strategies of the black hat community targeting multiple networks. These honeypots do not directly benefit a particular organization; instead, they investigate the threats organizations face and know how to help defend against such threats. Research honeypots are challenging to set up and preserve, collect a large amount of data and are mainly is used by military, research, or government organizations.

Honeypots are classified into three types based on their interaction:

•Low interaction honeypots: Low interaction honeypots provide the hacker with little to no knowledge and command over the network. It only simulates the services that the attackers frequently request. It is less risky, as its primary operating system is not involved in the low interaction systems. They require few resources and are simple to implement. The only disadvantage of these is that skilled hackers can quickly identify them and ignore them.
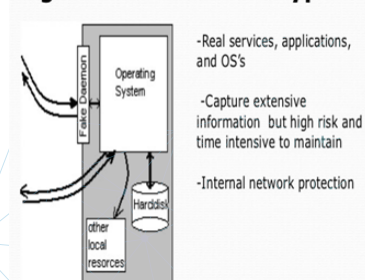

Low Interaction Honeypot..

-Emulates certain services, applications

-Identify hostile IP

-Protect internet side of network

-Low risk and easy to deploy/maintain, but capture limited information.

Security HoneyPOT
Scanning Attack

•High-interaction honeypots mimic the actions of production systems that support a wide range of services; as a result, the attacker may be granted access to a wide variety of services to waste their time. Multiple honeypots can be hosted on a single physical machine by using virtual machines. As a result, even if the honeypot is damaged, it can be recovered quite fast. High-interaction honeypots typically offer greater security by being hard to trace but are costly to maintain. If virtual machines are inaccessible, each honeypot must have its physical computer, which can be outrageously expensive.

•Honeypots in their purest form are full-fledged production systems. A bug tap is installed on the honeypot's network connection and is used to monitor the attacker's activities. There is no need to install any additional software. Although a pure honeypot is effective, a more controlled mechanism can ensure the stealth capabilities of the defense mechanisms.

High Interaction Honeypot...

-Real services, applications, and OS's

-Capture extensive information but high risk and time intensive to maintain
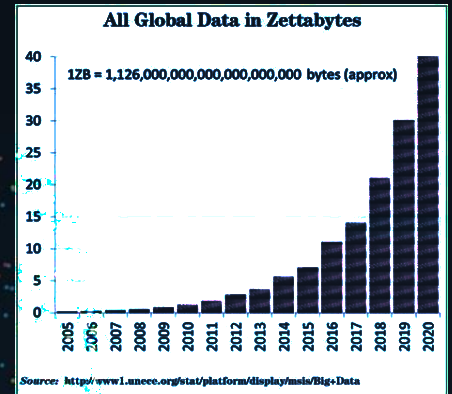
-Internal network protection

DATA MINING

by Lavaneeth Reddy

We have an abundant amount of data but starving for extracting meaning from that data. If we do gold mining or coal mining, you are digging for the gold or coal, whereas in data mining, you're not mining for the data, but you're mining for knowledge from the available data. So, data mining is also known as knowledge mining. Data mining is so important because there is a massive amount of data available; according to the statistics, the amount of data produced in the last three years is more than the total amount of data produced during the whole century.

Data mining is discovering hidden patterns from already available extensive data and can be available in different forms. It can be hard copy, soft copy, online records, and many more other formats. And that can help us find out some patterns some knowledge from the data, which is what data mining is all about—extracting knowledge from data that can be used to make effective decision making. It uses software, algorithms, and statistical methods to identify patterns in the data. There are five primary steps to data mining. 1. Identification of business issues to analyze data, such as databases or operational systems. 2. Data collection and exploration, which includes the sampling and profiling of the data sets. 3. Data preparation and transformation to filter, cleanse, and structure data for analysis. 4. Modeling, data scientists, and other users create, test, and evaluate data mining models. 5. Deployment of the models for analytics uses.

Data mining is used on various forms of data and is applied to find interesting patterns rather than results from the database. Data mining techniques are used in many business research areas like marketing, fraud detection, risk management, cyber security, medical diagnosis, and mathematics. Data mining is the most primarily used method in different data sources. It is one of the most booming methods that companies and organizations use, and the usage is widely going to increase in the future.

All Global Data in Zettabytes

1ZB = 1,126,000,000,000,000,000,000 bytes (approx)

*Source:* https://www1.unece.org/stat/platform/display/msis/Big+Data

OLED TECHNOLOGY

by Aparna vemuganti

The word OLED stands for Organic Light Emitting Diode, belongs to the family of LED's which consumes low power and is part of different combinations of colors. OLED technology uses the principle of electroluminescence, where certain materials emit light when we pass an electric current through them. OLED's display has many advantages, such as computer monitors, TV screens, digital cameras, and even mobile phones. The thickness of
these diodes is from 100 to 500 nanometers. It is 200 times smaller when compared to human hair. OLED displays are costly compared to LCD. However, OLED displays are beneficial as they are bright, clear, thin, light in weight, and possess an efficient viewing angle. In addition, OLED lights contain no mercury and thus eliminates the pollution problems in fluorescent lighting.
There are four layers in OLED: anode, cathode, emissive layer, and a conductive layer, where every layer has its importance.

TYPES OF OLED TECHNOLOGY:
Based on the structure of OLED, they are classified as:
Passive OLED, Active OLED, Transparent OLED, Top emitting OLED, White OLED, Foldable OLED.
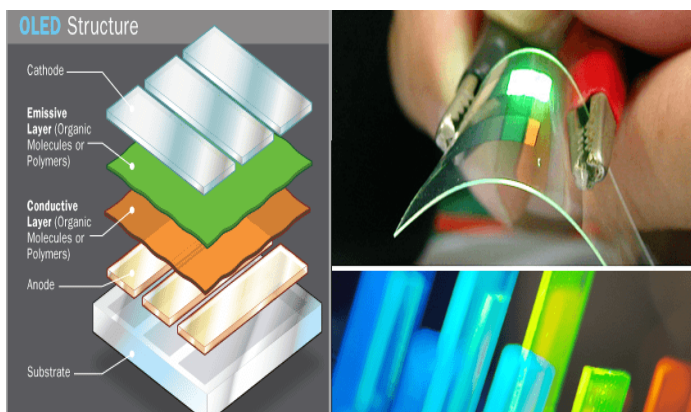
1. Passive OLED: These OLEDs which describe the external circuitry and pixel information are known as Passive OLEDs. These OLEDs are easy to make and use more power and best options for small screens.
2. Active-matrix OLED: These OLEDs require less power and are suitable for large-screen displays. An anode is used to control pixels.
3. Transparent OLED: These OLED types are helpful for heads-up displays, transparent projector screens, and glasses.
4. Top emitting OLED: These OLEDs are used with the active matrix devices and in the making of intelligent card displays.
5. White OLED: These OLEDs emit only white light and are used to make larger and efficient lighting systems.

These OLEDs replace the fluorescent lights, and the energy cost is reduced for lighting.
6. Foldable OLED: These OLEDs are made up of flexible metallic foil or plastic substrate. They are flexible and easily movable.
7. Phosphorescent OLED: This OLED works on electroluminescence, which converts 100 % of the electrical energy into light. These OLEDs reduce heat generation.
APPLICATIONS OF OLED TECHNOLOGY: There are several applications of OLED
•Television screens
•Cellphone screens
•Computer monitors
•Keyboards
•Lights
•Portable device displays

DATA SCIENCE

by Kenny Joel kuragayala

Data science is about making data actionable. It can be done in various forms, such as insights, product recommendations, and so on. Basically, as a data scientist, your job is to solve company problems using data.
Data science is the process of finding solutions to problems through the use of data. It involves analyzing and predicting how those solutions will perform.

So here we consider uber as a case study to know how data science is being used. Monday, we get to work before a meeting begins. So we go looking for taxis. So I open up Uber App and look for cabs. At this hour of the day, there's something unusual about the high fares. Monday mornings are usually when the cabs are driving around in peak hours, and people rush off to work. So naturally, this increases the prices of taxis. But how is all of this implemented?

Data science is at the core of the algorithm used by uber to set the prices of their rides. Its goal is to ensure that every passenger gets a ride whenever they need one. Data science is used by uber to determine which neighborhoods will be the busiest, and thus, how many rides will be provided to them. This algorithm uses data science to determine which areas will be the most populated and improve surge pricing. It increases the prices in the app in busy times. Understanding a business requirement or a problem is the first step in developing a data science process. The business model should be able to take advantage of the dynamic pricing system when many people are requesting rides in the same area.

It is followed by data collection, weather data, traffic data, drop location, and more are some of the things that uber collects. It keeps track of all of this and more.
The next step is data cleaning. It is a process that removes non-necessary data from the system. This step is usually carried out when a data collector collects data that is not needed to be collected in the first place, like restaurants, cafés, etc.
Then it is followed by data exploration and analysis. The data explora-

tion stage is where you get started analyzing and understanding the patterns in your data.
This is followed by the data modeling stage, where the model is built to predict the surge of an individual or a group based on their location. This model is created by combining the data collected during the exploratory stage with thousands of customer records. It learns to predict the outcome more accurately by feeding the records into it.

The validation stage is when the new customer data is compared with the previous data to see any anomalies. If there are any anomalies in the data collected by the company, they will be notified immediately and sent to the data scientists of the company. This shows how uber predicts a surge price based on a given location and time.
After testing the model, it is deployed to all the users. This step is the final step of the science. Again, feedback is received, and if there is any issue, it will be fixed here.
All that is data science process

CRYPTOCURRENCY
by Rushivardhan

Cryptocurrency is a digital or virtual currency created by computers performing conscientious mathematical computations and thereby changing electricity into long strings of code that have price. This computing is finished during a distributed network and is termed cryptocurrency mining.

Although not all cryptocurrencies are created in this manner, most of the distinguished ones are. The rule often used to mine cryptocurrencies is a decreasing-supply rule which limits cryptocurrencies exploitation encoding techniques.

To put it in straightforward terms, this sort of rule ensures that, like a lot and lot of the cryptocurrency is deep-mined, it becomes increasingly more complex and resource-intensive to mine. Once the availability of a currency is proscribed, it will facilitate to secure its worth. Thus, cryptocurrency mining becomes increasingly more complex and resource-intensive, similar to the mining of natural minerals.

The encoding techniques used to mine cryptocurrencies, including blockchain technology, don't facilitate the verification of fund transfers between users of a particular cryptocurrency.
Bitcoin Transactions Are:

1. Irreversible – when a bitcoin group action has been confirmed, no one can reverse it.
2. Low cost – A bitcoin group action will move thousands of bucks with a nominal group action cost, that is on the average but one U.S. dollar.
3. Quick – The speed at which transactions are often processed depends on the proportion of users the area unit is willing to pay. Bitcoin transactions will usually be confirmed in a couple of minutes.
4. World – Bitcoin is often sent to primarily anyone, anyplace within the world.

HOW CRYPTOCURRENCY WORKS

Cryptocurrencies mainly work by cryptographic protocols or highly complex code systems that write sensitive knowledge transfers to secure their exchange amounts. Cryptocurrency developers build these protocols on advanced arithmetic and pc engineering principles that make it nearly impossible to interrupt, duplicate, or counterfeit the protected currencies. A cryptocurrency's blockchain is the master public ledger that records and stores all previous transactions and activity, confirmatory possession of all currency units at any given purpose in time.

As the record of a cryptocurrency's entire group action history, blockchain encompasses a finite length, containing a limited range of transactions that will increase over time. Identical copies of the blockchain area unit are kept in each node of the cryptocurrency's software. In addition, the network of localized server farms, pass computers or teams called miners, regularly records and attests to cryptocurrency transactions.

Technically, a cryptocurrency group action isn't finalized until it's supplemental to the blockchain, which takes one to two minutes. However, once the group action is finalized, it's usually irreversible.

Unlike ancient payment processors, like PayPal and visa cards, credit cards, most cryptocurrencies don't have any integral refund or chargeback functions, and some newly developed crypted refund options. tocurrencies have initiated refund options.

During the lag time between the transaction's initiation and declaration, the units are not supposed to be used by either party. Instead, they control during a type of written agreement for all intents and functions.

Thus, the blockchain stops double-spending or copying cryptocurrency code to permit constant currency units to be duplicated and sent to multiple recipients.