UNIT1 BLOCKCHAIN BASICS

Basics of Crypto economics- Blockchain – Cryptocurrencies overloaded –Blockchain in Nutshell: Benefits and Challenges – Blockchain types - Blockchain Peer to Peer Network: Consensus Mechanisms, Proof of Work, Proof of Stake, Mining Layer, Propagation Layer, Semantic Layer, Application Layer

Basics of Crypto economics:

- Cryptoeconomics refers to the study of economic interaction in adversarial environments.
- The underlying challenge is that in decentralized P2P systems, that do not give control to any centralized party, one must assume that there will be bad actors looking to disrupt the system.
- Cryptoeconomic approaches combine cryptography and economics to create robust decentralized P2P networks that thrive over time despite adversaries attempting to disrupt them.
- The cryptography underlying these systems is what makes the P2P communication within the networks secure, and the economics is what incentivizes all actors to contribute to the network so that it continues to develop over time.
- Before the advent of Bitcoin, it was commonly believed to be impossible to achieve fault-tolerant and attack resistant consensus among nodes in a P2P network (Byzantine General's Problem).
- Satoshi Nakamoto introduced economic incentives to a P2P Network and solved that problem in the Bitcoin White Paper published in 2008.
- While decentralized P2P systems based on cryptography were nothing new – see Kazaa and BitTorrent – what these P2P systems before Bitcoin lacked was the economic incentive layer for coordination of the network of participants.
- Satoshi's implementation of a Proof of Work (POW) consensus mechanism introduced a new field of an economic coordination game, now referred to as cryptoeconomics.
- The underlying challenge of P2P networks of untrusted actors is how to deal with malicious network nodes in the absence of centralized parties securing the system.
- This is referred to as the "Byzantine Generals Problem." A malicious node, also called a Byzantine node, can lie and intentionally mislead other nodes involved in the consensus process.

- One must always assume that there will be bad actors trying to disrupt any open and public network.

- How can such a distributed network reach consensus about which data is correct or which is not correct, or which process is true or false in such an untrusted setup? Byzantine failures are considered the most difficult class of failures in distributed networks.

- Reliable consensus mechanisms must have sufficient resilience to withstand DDoS (Distributed Denial of Service) attacks, "Sybil attacks,"11 and other cyber attacks.
- They must also meet "Byzantine Fault Tolerance" requirements.

- Before Bitcoin, it was believed to be impossible to achieve fault-tolerant and attack-resistant consensus among untrusted nodes in a P2P network.

Fault-Tolerant:
Decentralized systems are less likely to fail accidentally because they rely on many separate components.

Attack-Resistant:
Decentralized systems are more expensive to attack and destroy or manipulate because they lack sensitive central points that can be attacked at much lower cost than the economic size of the surrounding system.

Collusion-Resistant:
It is much harder for participants in decentralized systems to collude and act in ways that benefit them at the expense of other participants, whereas the leadership of corporations and governments collude in ways that benefit themselves but harm less well-coordinated citizens, customers, employees and the general public all the time.

Network Security: Cryptoeconomic Mechanisms

- "Proof-of-Work" is the consensus mechanism of the Bitcoin Network and similar blockchain networks.

- It is a set of rules and processes that define how multiple nodes can reach an agreement on the true state of the network.

- It is designed in a way that if you spend money, and you play fair by the rules, you can make money.

- It doesn't pay to cheat. In this setup, the miners, or mining computers, validate transactions and compete with each other to calculate a cryptographic hash of the next block.

- This competition is driven by a cryptographic puzzle where all miners compete to be the first to find a solution to a mathematical problem, where they have to find an input that gives a specific hash value.

- Miners hereby have to collect recent transactions and some metadata, verify the transactions, and run all the data through a SHA-256 algorithm.
- They must find a hash value which begins with a consecutive number of zeros. This means that they have to perform computational work to solve the puzzle, which is the reason why this process is referred to as "Proof-of-Work."
- The first miner that solves a mathematical puzzle can write transactions to the blockchain, creating the next block, and in return, they get a "block reward" for the costs incurred in the form of new network tokens.

- In the case of the Bitcoin Network, it would be Bitcoin (BTC); in the Ethereum Network, it is Ether (ETH).

- This means that all network participants that work toward adding blocks of transactions to the ledger can potentially earn network tokens (block reward plus potential transaction fees).

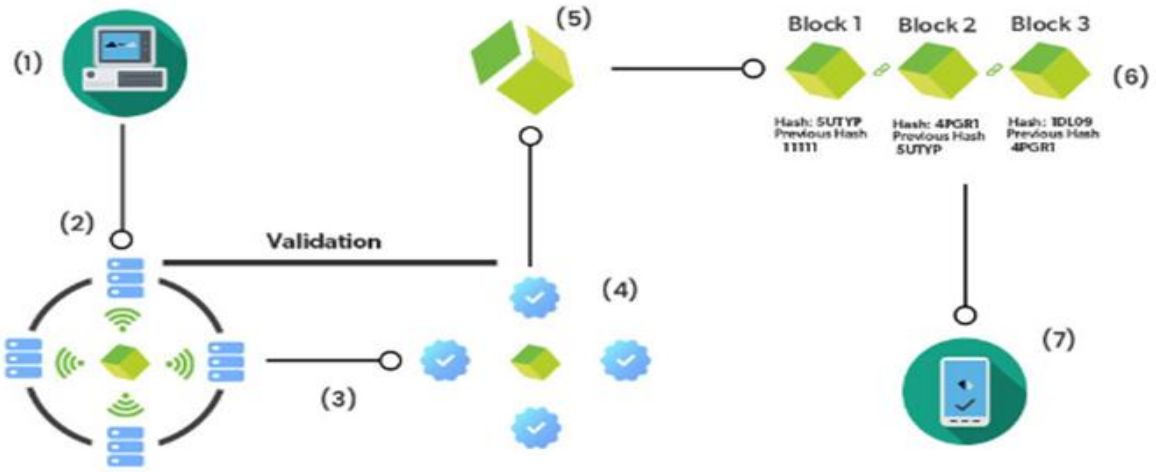
- At the time of writing this book, the reward for successful block creation in the Bitcoin Network is 12.5 BTC per block.

- The block reward gets reduced by 50 percent every 210.000 blocks, around every four years. The next "halving" of block rewards is in 2020.

- By participating in this race, miners collectively make sure that all transactions included in a block are valid.

- To get a better understanding of how high economic costs of attacking or manipulating a network would be, it is helpful to check these websites, because they provide real-time information about how much it currently costs to attack blockchains and similar networks.

Crypto-Economics Model:



1. Transaction Request: Someone requests a transaction. In the case of Blockchain, a transaction is requested using a device known as a wallet. A cryptoeconomics wallet is a type of digital wallet that allows users to store and manage the cryptocurrencies like bitcoin and ether.

2. Transaction Broadcast: The requested transaction is then broadcasted in a Peer to Peer network consisting of computers, which are also known as nodes. Peer-to-peer (P2P) networking connects a group of computers with equal data processing rights and responsibilities. Unlike traditional client-server networking, no devices in a P2P network are completely dedicated to serving or receiving data.

3. Transaction Validation: After the transaction has been broadcasted to all the nodes in the network, the network of nodes validates the transaction and the user's status. In other words, once a transaction is delivered to any node connected to the network, the transaction will be verified by that node. If the transaction is found to be legitimate, then that node will disseminate it to the other nodes to whom it is linked, and a success message will be delivered synchronously to the originator.

4. Verification Process: Bitcoin uses digital signatures established using keypairs to authenticate transactions and senders. The sender wants to guarantee that the proper bitcoin amount is transmitted to the correct individual (wallet), and the receiver wants to check that the data is valid and from the sender. The data to be delivered was gathered by the sender. A verified transaction can involve cryptocurrency contracts, records, or other information.

5. Block Formation: After the verification is done, the transaction is combined with other transactions. To create a new block of data for the ledger. A bitcoin public ledger is a mechanism for keeping track of transactions. The ledger anonymously stores individuals' names, cryptocurrency balances, and a record of all authentic transactions completed between network participants.

6. Adding the block to the blockchain: The new block is then added to the existing blockchain in a way that is permanent and unalterable. The ledger is spread among numerous nodes, which means that data is copied and saved in real-time on each node in the system. When a transaction is registered in the blockchain, data like as the transaction's price, asset, and ownership are recorded, validated, and settled across all nodes in seconds.

7. Transaction Complete: Then, the transaction is finally complete

Block Chain

- A blockchain is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

- Blockchain has been in a lot of buzz these days and that is mainly because it is backbone of the very famous cryptocurrency in the world - the Bitcoin.

- Many Governments and leading Banks have decided to bring many of their conventional transactions based on Blockchain concept.
- The applications and potential of this framework is huge and is considered to be changing the way transactions are made in various domains.

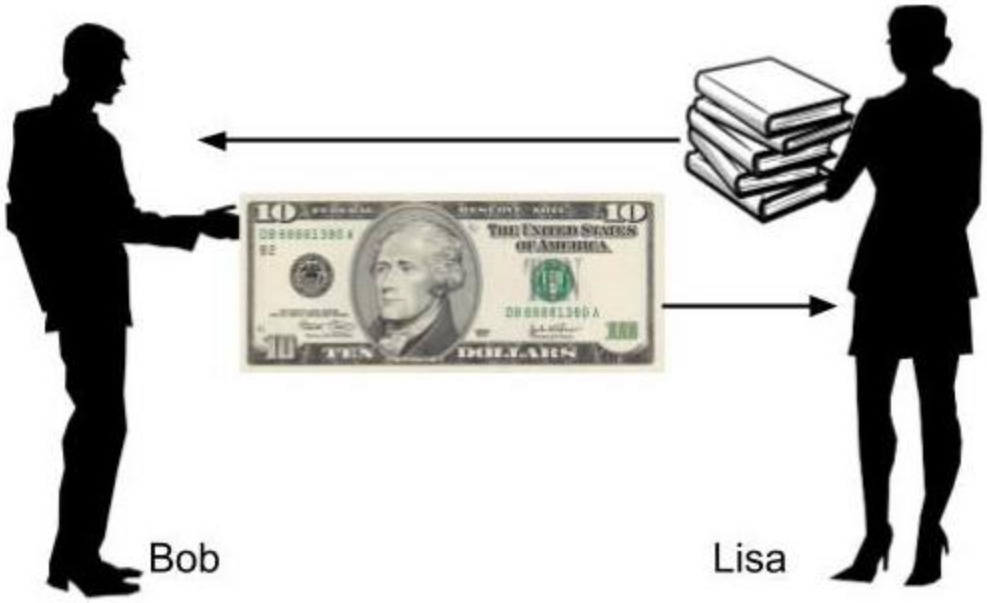
- Many have described this as a most disruptive technology of the decade. Especially, the financial markets could be the most affected ones.

- The technology is being adapted into many verticals like Healthcare, Medicines, Insurance, Smart Properties, Automobiles, and even Governments.

- However, so far the most successful implementation of Blockchain is the Bitcoin - A Peer-to-Peer Electronic Cash System, which incidentally is also the first implementation of blockchain technology. Thus, to understand blockchain technology, it is best to understand how Bitcoin System is designed and implemented.

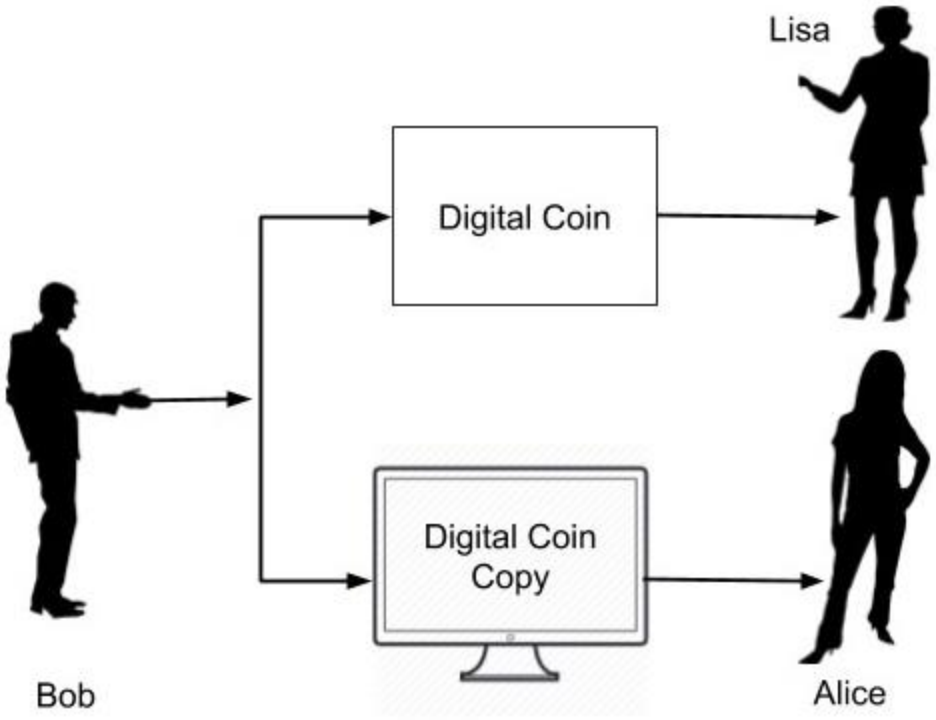
Emergence of Block chain: Double- Spending

Consider a situation shown in image –

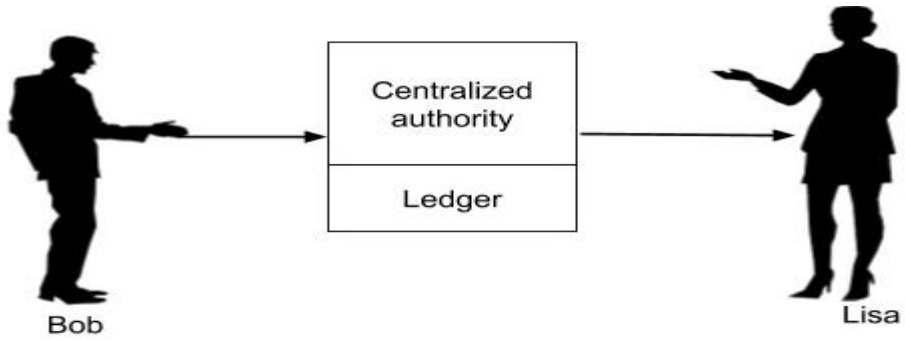


As clearly seen here, Bob is tendering a $10 bill to Lisa in exchange of a book. Once the Lisa receives this physical $10 bill, there is no way for Bob to re-use this money for some other transaction, as the physical currency is now in Lisa's possession.

Now, consider a situation where the money is paid in Digital form. This is illustrated in image –



- As the format for money exchange is in the digital format, it is essentially a binary physical file stored somewhere on Bob's device.
- After Bob gives this file (digital money) to Lisa, he can also a give a copy of the file to Alice.
- Both now think that they have received the money without having any means of authenticating the digital coin and would thus deliver their respective goods to Bob.
- This is called double-spending where the sender spends the same money at more than one place for obtaining services or goods from multiple vendors.
- To solve this problem of double-spending, one would employ a centralized authority to monitor all the transactions.



- The centralized authority, which in common terms is your bank, maintains a ledger book recording all the transactions. Now, Bob has to send his digital money to the bank who would make an entry into its ledger debiting Bob's account.
- After ensuring that Bob has sufficient balance to pay for the digital money which he wants to send, would send the money to Lisa crediting her account in its ledger.
- Now, it is guaranteed that Bob cannot double spend the money.
- If every digital transaction is routed through a centralized authority like this, the problem of double-spending would be solved.
- This also provides another benefit in validating the authenticity of each coin (digital money) that it receives in the transaction.
- So the fake money (duplicate money as in the case of Bob paying to Alice using a copy) would be easily detected and prevented from the circulation.
- The introduction of centralized authority though it solves the double-spending problem, introduces another major issue - the cost of creating and maintaining the centralized authority itself.
- As the banks need money for their operations, they start cutting commissions on each currency transaction they do for their clients. This sometimes can become very expensive, especially in overseas transfer of money where multiple agents (banks) may be involved in the entire deal.
- All the above issues are solved by the introduction of digital currency, called **Bitcoin.**

Cryptocurrencies Overloaded:

Cryptocurrencies have become increasingly popular over the past several years - as of 2018, there were more than 1,600 of them! And the number is constantly growing. With that has come to an increase in demand for developers of the blockchain (the underlying technology of cryptocurrencies such as bitcoin). The salaries blockchain developers earn show how much they are valued: According to Indeed, the average salary of a full-stack developer is more than $112,000.

History of Cryptocurrency

In the caveman era, people used the barter system, in which goods and services are exchanged among two or more people. For instance, someone might exchange seven apples for seven oranges. The barter system fell out of popular use because it had some glaring flaws:

- People's requirements have to coincide—if you have something to trade, someone else has to want it, and you have to want what the other person is offering.
- There's no common measure of value—you have to decide how many of your items you are willing to trade for other items, and not all items can be divided. For example, you cannot divide a live animal into smaller units.
- The goods cannot be transported easily, unlike our modern currency, which fits in a wallet or is stored on a mobile phone.

After people realized the barter system didn't work very well, the currency went through a few iterations: In 110 B.C., an official currency was minted; in A.D. 1250, gold-plated florins were introduced and used across Europe; and from 1600 to 1900, the paper currency gained widespread popularity and ended up being used around the world. This is how modern currency as we know it came into existence.

Traditional Currencies vs. Cryptocurrencies

Imagine a scenario in which you want to repay a friend who bought you lunch, by sending money online to his or her account. There are several ways in which this could go wrong, including:

- The financial institution could have a technical issue, such as its systems are down or the machines aren't working properly.
- Your or your friend's account could have been hacked—for example, there could be a denial-of-service attack or identity theft.
- The transfer limits for your or your friend's account could have been exceeded.

There is a central point of failure: the bank.

- This is why the future of currency lies with cryptocurrency.
- Now imagine a similar transaction between two people using the bitcoin app.
- A notification appears asking whether the person is sure he or she is ready to transfer bitcoins.
- If yes, processing takes place: The system authenticates the user's identity, checks whether the user has the required balance to make that transaction, and so on.
- After that's done, the payment is transferred and the money lands in the receiver's account. All of this happens in a matter of minutes.

- Cryptocurrency, then, removes all the problems of modern banking:

- There are no limits to the funds you can transfer, your accounts cannot be hacked, and there is no central point of failure.

- As mentioned above, as of 2018 there are more than 1,600 cryptocurrencies available; some popular ones are Bitcoin, Litecoin, Ethereum, and Zcash.

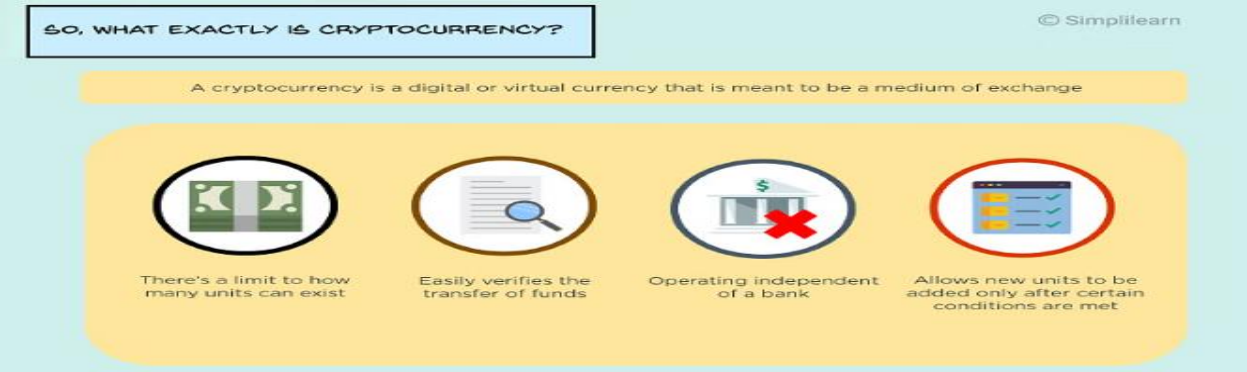
- And a new cryptocurrency crops up every single day. Considering how much growth they're experiencing at the moment, there's a good chance that there are plenty more to come!

- Modern currency includes paper currency, coins, credit cards, and digital wallets—for example, Apple Pay, Amazon Pay, Paytm, PayPal, and so on. All of it is controlled by banks and governments, meaning that there is a centralized regulatory authority that limits how paper currency and credit cards work.

Definition- cryptocurrency

A cryptocurrency is a digital or virtual currency that is meant to be a medium of exchange. It is quite similar to real-world currency, except it does not have any physical embodiment, and it uses cryptography to work.

Because cryptocurrencies operate independently and in a decentralized manner, without a bank or a central authority, new units can be added only after certain conditions are met. For example, with Bitcoin, only after a block has been added to the blockchain will the miner be rewarded with bitcoins, and this is the only way new bitcoins can be generated. The limit for bitcoins is 21 million; after this, no more bitcoins will be produced.



Benefits of Cryptocurrency

- With cryptocurrency, the transaction cost is low to nothing at all—unlike, for example, the fee for transferring money from a digital wallet to a bank account.

- You can make transactions at any time of the day or night, and there are no limits on purchases and withdrawals.

- And anyone is free to use cryptocurrency, unlike setting up a bank account, which requires documentation and other paperwork.

- International cryptocurrency transactions are faster than wire transfers too.

- Wire transfers take about half a day for the money to be moved from one place to another. With cryptocurrencies, transactions take only a matter of minutes or even seconds.

Cryptocurrencies-Overloaded:

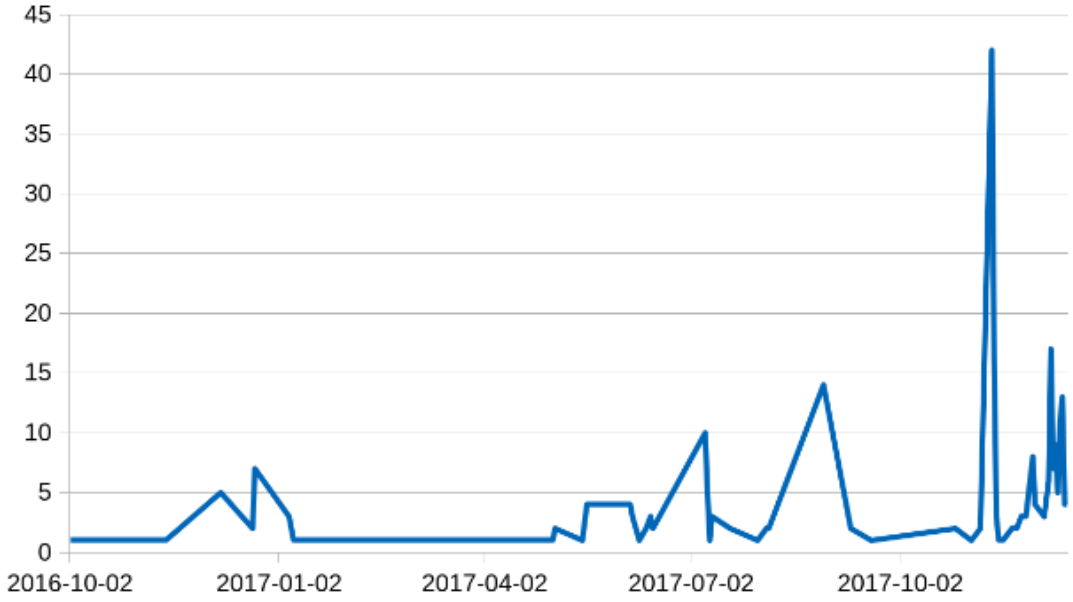
Like most high-visibility business, coin exchanges have been targeted with DDoS attacks. With the surge in interest and the resulting increase of traffic around cryptocurrencies, the door has been opened for bad actors to attempt to disrupt cryptocurrency resources, denying cryptocoin users access.

A distributed denial-of-service (DDoS) attack is one of the primary methods of disruption in the modern Internet. By overloading a target with bogus traffic, a bad actor is able to render a website or service unavailable. The popularity and importance of cryptocurrencies makes them a prime target for attack.

We've been analyzing some of the DDoS attacks hitting the many coin exchanges on our network in order to gauge any discernible patterns of interest. The most prominent volume of DDoS traffic originated from SSDP amplification attacks, NTP amplification attacks, and application layer attacks.

One popular coin exchange service has been flagged for 76 application layer DDoS attacks over about a year, though it's worth noting that the incredible surge in traffic may create false positives where normal traffic may show some signs of being an attack. Regardless, it's clear that bitcoin exchanges have become prime targets for DDoS.

Here's a graph showing the number of potential application layer attacks targeting popular cryptocurrency web properties through mid December 2017.



- Of particular interest is the huge spike in attacks around November 11.
- During this time a number of blockchain currency provider sites appear to have been targeted. Luckily, our DDoS mitigation software and infrastructure were able to prevent service disruption.

- Even in the best of circumstances, many of the websites and applications related to bitcoin and other cryptocurrencies do not have the resources to deal with a massive surge in traffic.
- Such increases can occur during a DDoS attack or during high levels of normal activity, resulting in temporary outages and denial-of-service.
- Hosting content on a CDN can be essential to keeping a site online, though it may also take a properly load balanced network of servers to be able to handle the number of database requests a surge can produce.
- Here's a graph showing the number of potential application layer attacks targeting popular cryptocurrency web properties through mid December 2017.

BLOCKCHAIN, the core technology behind the cryptocurrency bitcoin, is gaining publicity and interest from the financial-services industry, and other sectors are starting to take note of its potential disruption.

A blockchain is in essence a "digital ledger" where identical copies of all transactions are maintained in a network of computers controlled by different entities, which you may think of as a peer-to-peer network.

Trust is facilitated through the collective record-keeping maintained by each computer (node) ensuring the security and accuracy of the distributed ledger. Transactions are logged in an encrypted form that can be reviewed by participating nodes and entries are only allowed by a consensus of participants and can never be erased.

The key features and corresponding benefits of blockchain are:

- Its benefits include a decentralised and distributed approach to record keeping, and reliability and availability resulting from a large network of nodes sharing a blockchain and no single point of failure, thus making it resilient against outages and attacks.
- It provides an irreversible and immutable policy for transaction entries. Transparency,increasing auditability and trust as all transactions are visible and irrevocable, so changes cannot be made without detection, reducing opportunities for fraud.

- It allows near-real-time settlement of recorded transactions. Transactions can be verified and settled in minutes, reducing time needed to transfer funds or complete transactions.
- In considering the features and benefits of blockchain, the potential challenges arising from this technology should also be evaluated before further exploration.

- The greatest uncertainty surrounding blockchain is the commercial application of the technology and its regulation. Investments are flowing into exploring the concepts and potential applications of blockchain in every industry.
- The greatest amount of interest and activity is coming from the financial-services industry, exploring applications for both public and permission blockchains. Three types of blockchains currently exist.

Public blockchain: for example the bitcoin blockchain that anyone can read, transact and

validate through a consensus.

Consortium blockchain: for example R3, a consortium of financial institutions with a preselected set of nodes to control the consensus process.

Private blockchain: with write permissions centralised to an organisation but read permission can be public or restricted.

- Blockchain seems to be a promising way to reduce the risks in securities trading with almost no latency in settlement, which helps simplify middle and back-office processes.

- Other industries are exploring the application of blockchain for securely storing medical records, recording contracts, accruing loyalty points and more.
- How the technology is going to be adopted across industries is still uncertain, as most applications currently use case being tested and prototyped.
- Organisations should realise that as with all digital technologies that have enabled greater efficiency in processes, blockchain has the same potential to transform industries with its distributed ledger technology to simplify processes further, save money and minimise risks of fraud or unreliability.

Blockchain types:

There are three types of blockchain

- ***Public blockchain.***

  A public, or permission-less, blockchain network is one where anyone can participate without restrictions. Most types of cryptocurrencies run on a public blockchain that is governed by rules or consensus algorithms.

Examples of public blockchain: Bitcoin, Ethereum, Litecoin, NEO

Advantages

Public blockchains are good at what they do. Its advantages include the following.

- Anyone can join the public blockchain.
- It brings trust among the whole community of users
- Everyone feels incentivized to work towards the betterment of the public network
- Public blockchain requires no intermediaries to work.
- Public blockchains are also secure depending on the number of participating nodes
- It brings transparency to the whole network as the available data is available for verification purposes.

Disadvantages:

Public blockchain does suffer from disadvantages. They are as follows:

- They suffer from a lack of transaction speed.
- It can take a few minutes to hours before a transaction is completed.
- For instance, bitcoin can only manage seven transactions per second compared to 24,000 transactions per second done by VISA.
- This is because it takes time to solve the mathematical problems and then complete the transaction.
- Another problem with public blockchain is scalability. They simply cannot scale due to how they work.
- The more nodes join, the clumsier, and slow the network becomes. There are steps taken to solve the problem.
- For example, Bitcoin is working on lighting the network, which takes transactions off-

chain to make the main bitcoin network faster and more scalable.

- The last disadvantage of a public blockchain is the consensus method choice.
- Bitcoin, for example, uses Proof-of-Work (PoW), which consumes a lot of energy.
- However, this has been partially solved by using more efficient algorithms such as Proof-of-Stake (PoS).

- ***Permissioned or private blockchain.***

  A private, or permissioned, blockchain allows organizations to set controls on who can access blockchain data. Only users who are granted permissions can access specific sets of data. Oracle Blockchain Platform is a permissioned blockchain.

  Examples of Private blockchain: Multichain, Hyperledger Fabric, Hyperledger Sawtooth, Corda

  Advantages:

  - Private blockchains are fast. This is because there are few participants compared to the public blockchain. In short, it takes less time for the network to reach consensus resulting in faster transactions.

  - Private blockchains are more scalable. The scalability is possible because, in a private blockchain, only a few nodes are authorized to validate transactions. This means it doesn't matter if the network grows; the private blockchain will work at its previous speed and efficiency. The key here is the centralization aspect of decision making.

  Disadvantages:

  - Private blockchains are not truly decentralized. This is one of the biggest disadvantages of private blockchain and goes against the core philosophy of distributed ledger technology or blockchain in general.
  - Achieving trust within the private blockchain is tough because the centralized nodes make the last call.
  - Lastly, as there are only a few nodes here, the security isn't all that good. It is important to understand that it is possible to lose security if a certain number of nodes go rogue and compromise the consensus method utilized by the private network.

- ***Federated or consortium blockchain.***

  A blockchain network where the consensus process (mining process) is closely controlled by a preselected set of nodes or by a preselected number of stakeholders.

  Examples of Consortium Blockchain: Marco Polo, Energy Web Foundation, IBM Food Trust.

Advantages:

- It offers better customizability and control over resources.
- Consortium blockchains are more secure and have better scalability.
- It is also more efficient compared to public blockchain networks.
- Works with well-defined governance structures.
- It offers access controls.

Disadvantages:

- Even though it is secure, the whole network can be compromised due to the member's integrity.
- It is less transparent.
- Regulations and censorship can have a huge impact on network functionality.
- It is also less anonymous compared to other types of blockchain.

Hybrid Blockchain

Hybrid blockchain is one of the different types of blockchain technology. More so, Hybrid blockchain is the last type of blockchain that we are going to discuss here. More so, hybrid blockchain might sound like a consortium blockchain, but it is not. However, there can be some similarities between them.

Hybrid blockchain is best defined as a combination of a private and public blockchain. It has use-cases in an organization that neither wants to deploy a private blockchain nor public blockchain and simply wants to deploy both worlds' best.

Example of Hybrid Blockchain: **Dragonchain, XinFin's Hybrid blockchain**

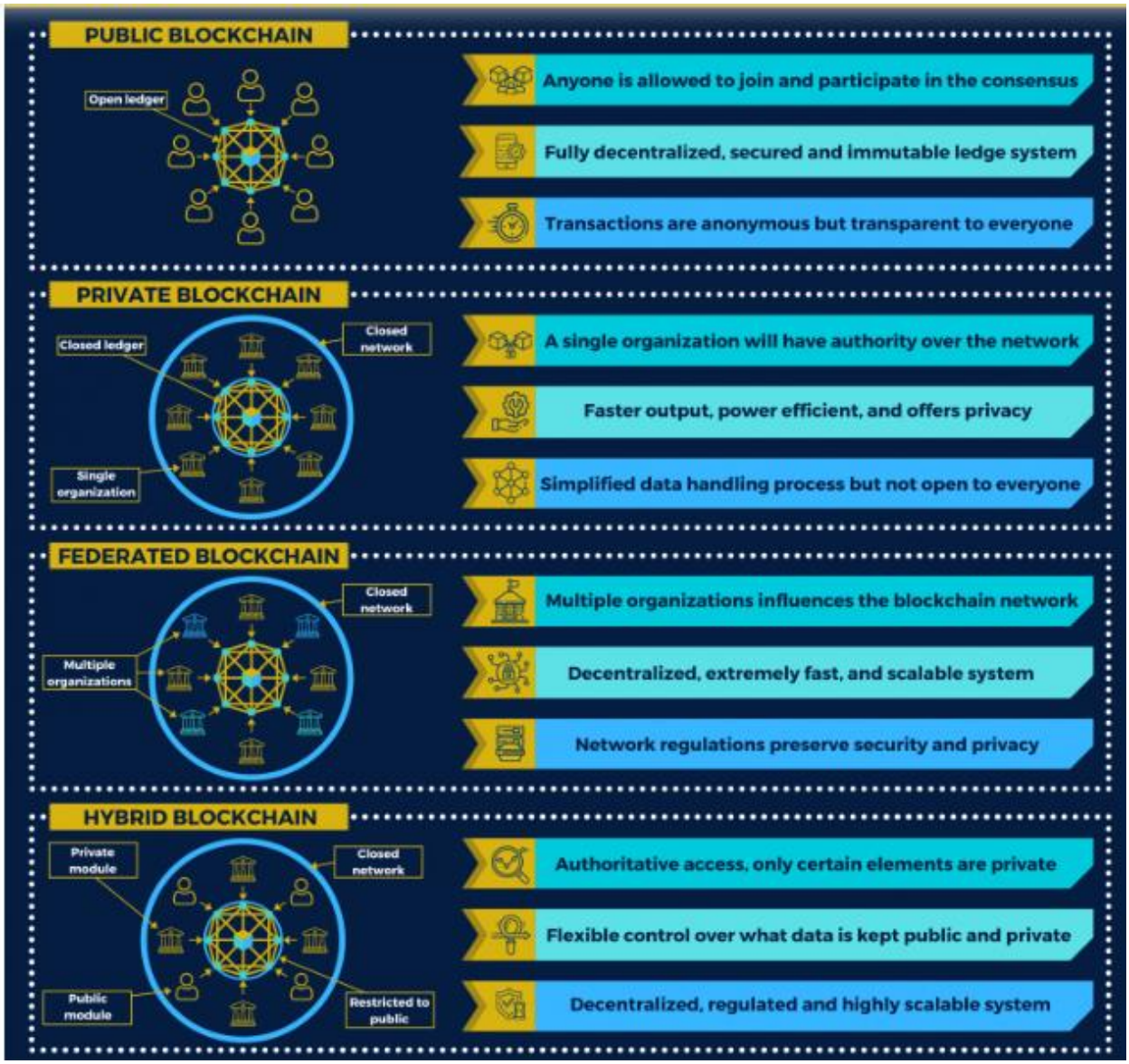
Advantages:

- Works in a closed ecosystem without the need to make everything public.
- Rules can be changed according to the needs.
- Hybrid networks are also immune to 51% attacks.
- It offers privacy while still connected with a public network.
- It offers good scalability compared to the public network.

Disadvantages:

- Not completely transparent.

- Upgrading to the hybrid blockchain can be a challenge.
- There is no incentive for participating and contributing to the network.



Blockchain Peer to Peer Network:

- P2P is a technology that is based on a very simple principle, and that is the concept of decentralization.

- The peer-to-peer architecture of blockchain allows all cryptocurrencies to be transferred worldwide, without the need of any middle-man or intermediaries or central server.

- With the distributed peer-to-peer network, anyone who wishes to participate in the process of verifying and validating blocks can set up a Bitcoin node.

- Blockchain is a decentralized ledger tracking of one or more digital assets on a peer-to-peer network.

- When we say a peer-to-peer network, it means a decentralized peer-to-peer network where all the computers are connected in some way, and where each maintains a complete copy of the ledger and compares it to other devices to ensure the data is accurate.

P2P: Pros & Cons

Let's talk about the advantages first. Here are few undeniable benefits of the P2P network in the blockchain.

- As blockchain is a decentralized system of peer to peer network, it is highly available due to decentralization.Because of P2P networking capability, even if one peer gets down, the other peers are still present. Thus nobody can take down the blockchain.

- P2P networks offer greater security compared to traditional client-server systems.

- When you are using cloud computing to store your data, you need to trust AWS and Google drives, but with the blockchain, because it utilizes peer to peer network you don't need to trust any third parties which can modify your crucial data. These are non-resistant to censorship by central authorities.

- These networks are virtually immune to the Denial-of-Service (DoS) attacks.

- The distributed peer-to-peer network, when paired with a majority consensus requirement, gives blockchains a relatively high degree of resistance to malicious activity.

- P2P network in blockchain, however, raises few concerns. As in blockchain, instead of a central server, distributed ledgers must be updated on every single node, adding transactions requires a considerable amount of computational power.

- Although this provides an increased level of security, it significantly reduces efficiency, and this acts as one of the main hindrances in terms of scalability and mass adoption.

From file-sharing networks to energy trading platforms, the P2P system can serve several other distributed computing applications. P2P is the core of the blockchains that make cryptocurrencies possible as its architecture offers decentralization, security and eradicates dependencies on third-party.

Consensus Mechanisms:

A consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies. It is useful in record-keeping, among other things.

On the Bitcoin blockchain, for instance, the consensus mechanism is known as Proof-of-Work (PoW), which requires the exertion of computational power in order to solve a difficult but arbitrary puzzle in order to keep all nodes in the network honest.

In any centralized system, like a database holding key information about driving licenses in a country, a central administrator has the authority to maintain and update the database. The task of making any updates—like adding/deleting/updating names of people who qualified for certain licenses—is performed by a central authority who remains the sole in-charge of maintaining genuine records.

Public blockchains that operate as decentralized, self-regulating systems work on a global scale without any single authority. They involve contributions from hundreds of thousands of participants who work on verification and authentication of transactions occurring on the blockchain, and on the block mining activities.

In such a dynamically changing status of the blockchain, these publicly shared ledgers need an efficient, fair, real-time, functional, reliable, and secure mechanism to ensure that all the transactions occurring on the network are genuine and all participants agree on a consensus on the status of the ledger. This all-important task is performed by the consensus mechanism, which is a set of rules that decides on the legitimacy of contributions made by the various participants (i.e., nodes or transactors) of the blockchain.

Blockchain Consensus Mechanisms

There are different kinds of consensus mechanism algorithms, each of which works on different principles.

The **proof of work (PoW)** is a common consensus algorithm used by the most popular cryptocurrency networks like bitcoin and litecoin. It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain. However, this whole mining mechanism of bitcoin needs high energy consumption and a longer processing time.

The **proof of stake (PoS)** is another common consensus algorithm that evolved as a low-cost, low-energy consuming alternative to the PoW algorithm. It involves the allocation of responsibility in maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens held by it. However, this comes with the drawback that it incentivizes cryptocoin hoarding instead of spending.

While **PoW and PoS** are by far the most prevalent in the blockchain space, there are other consensus algorithms like Proof of Capacity (PoC) which allow sharing of memory space of the contributing nodes on the blockchain network. The more memory or hard disk space a node has, the more rights it is granted for maintaining the public ledger. Proof of Activity (PoA), used on the Decred blockchain, is a hybrid that makes use of aspects of both PoW and PoS. Proof of Burn (PoB) is another that requires transactors to send small amounts of cryptocurrency to inaccessible wallet addresses, in effect "burning" them out of existence.

Another, called **Proof of History (PoH),** developed by the Solana Project and similar to Proof of Elapsed Time (PoET), encodes the passage of time itself cryptographically to achieve consensus without expending many resources.

Layers in Block Chain:

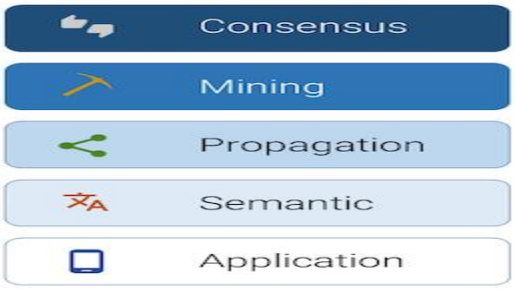
Blockchain itself should be decomposed into separate layers in order to better understand the security and economics of Blockchain design.

- Layered system design is best exemplified in the Internet.
- Each layer is more abstract than the lower layer, until we get to the physical transport layer.
- This approach allows for robust system design because each layer can be upgraded, patched, or even completely swapped out without affecting other layers.

Summary:

- The physical layer: the actual medium that transports the bits whether it be wireless spectrum, cable fiber, or phone lines.
- The network layer: manages addressing and routing of packets between different physical routers, most commonly IP.
- The transport layer: manages raw connection state, most commonly TCP.
- The session layer: manages higher level connection state, such as HTTP.
- The application layer: where actual applications live, e.g. Google search, Facebook, etc.

A Bitcoin layer decomposition



- **Consensus layer:** a protocol that describes the format of a ledger that is publicly visible and a consensus function that anyone can use to determine which of multiple candidate ledgers is the consensus ledger. The protocol must also allow new blocks to be added to the ledger.
- **Mining layer:** a protocol that incentivizes parties to maintain the consensus and add blocks to the ledger.

- **Propagation layer**: a protocol that determines how the ledger and blocks are transmitted between nodes in the network.
- **Semantic layer:** a specification of how new blocks must relate to previous blocks and a protocol for verifying conformity with the specification.
- **Application layer:** application code that implements some desired functionality.

The first four layers encompass what we think of as the Blockchain, while the application layer allows for overlays, APIs, applications, etc.

Properties

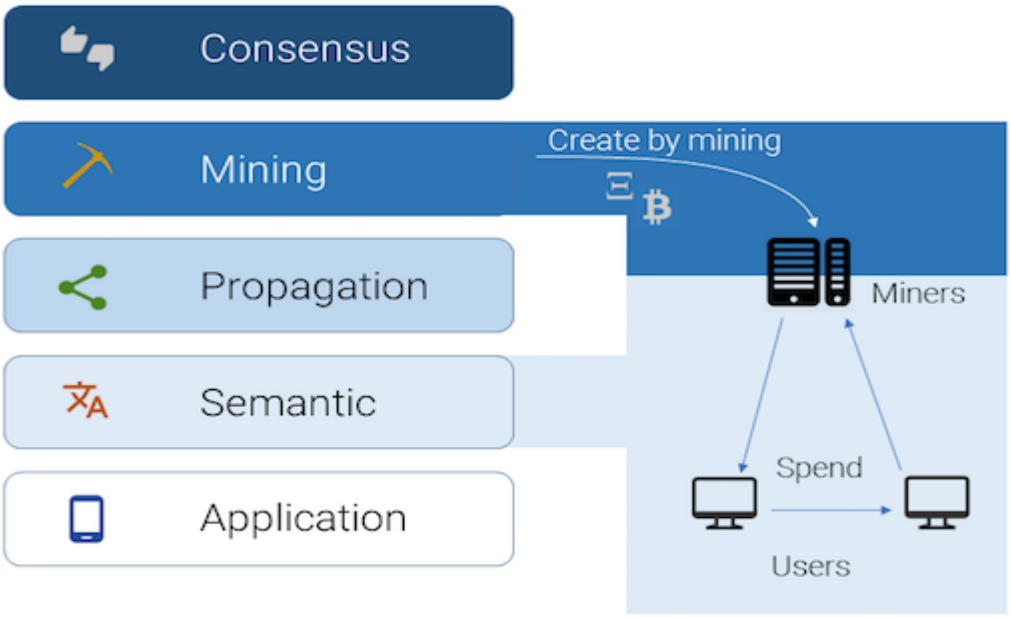
- **Security:** no party who doesn't control a majority of some scarce resource (typically computing power) can convince nodes that an alternate version of the ledger is the consensus
- **Liveness:** nodes can add new blocks to the ledger with acceptable latency
- **Stability:** nodes in the network should not alter their opinion of the consensus ledger (except in very rare cases)
- **Correctness:** only blocks that represent valid transactions (i.e. they conform to a specification of how new blocks may relate to previous blocks) may be added to the ledger

Our classification into four layers is natural because it's quite easy to identify that each of these properties is achieved primarily at one layer of our decomposition:

- **Security** is achieved at the **consensus layer**, and requires building a consensus function that cannot be fooled into accepting an alternate ledger without using a majority of all existing resources
- **Liveness** is achieved at the **mining layer**, and requires there to be enough incentive for participants in the network to continually confirm new blocks
- **Stability** is achieved at the **propagation layer**, and requires nodes to be able to quickly disseminate confirmed blocks to other nodes so that they know to build on the most recent blocks instead of older, stale blocks
- **Correctness** is achieved at the **semantic layer**, where blocks have a meaning, which could range from sending currency between parties as in Bitcoin to encoding state transitions in a state machine as in Ethereum, and where this meaning is validated by nodes to conform to the specification stating how new blocks must relate to previous blocks

Layer in which cryptocurrency live :

- Because existing Blockchains including Bitcoin and Ethereum work at all four layers (consensus+mining+propagation+semantic) simultaneously, it's not immediately clear at which layer cryptocurrency "lives". In fact, it lives at two layers and in two different forms. This fact is implicit in Bitcoin and explicit in Ethereum.



The mining layer: Bitcoins and Ether are created and/or transferred as valid blocks are created and added to the ledger. The currency is either generated from the network itself ("out of thin air") or taken from the transactions contained in the block ("transaction fees"). The currency is used to maintain an incentive for miners to hash blocks.

The semantic layer: Bitcoins and Ether can be transferred among nodes at the semantic layer by creating valid transactions signed by the holders of the cryptocurrency or by creating smart contracts that transfer the cryptocurrency between accounts. Here the cryptocurrency is used as a store of value and means of payment.

Since Ethereum is a general-purpose VM, you can also create alternate cryptocurrencies at the semantic layer to be used in the application layer. For example, DAO tokens functioned this way. These alternate cryptocurrencies live only at the semantic and application layers.