1. a) What is Blockchain? What are its key elements of blockchain?

Ans 1. a)

Blockchain

- **Blockchain is a type of shared database that differs from a typical database in the way that it stores information; blockchains store data in blocks that are then linked together via cryptography.**
- **As new data comes in, it is entered into a fresh block. Once the block is filled with data, it is chained onto the previous block, which makes the data chained together in chronological order.**
- **Different types of information can be stored on a blockchain, but the most common use so far has been as a ledger for transactions.**
- **In Bitcoin's case, blockchain is used in a decentralized way so that no single person or group has control—rather, all users collectively retain control.**
- **Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.**

Key elements of a blockchain:

1. **Distributed ledger technology**
   All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.
2. **Immutable records**
   No participant can change or tamper with a transaction after it's been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.
3. **Smart contracts**
   To speed transactions, a set of rules — called a smart contract — is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more.

1. b) Explain the Core Components of Blockchain Architecture.

Ans 1. b)

Core Components of Blockchain Architecture

- **Node: Nodes are network participants and their devices permit them to keep track of the distributed ledger and serve as communication hubs in various network tasks. A block broadcasts all the network nodes when a miner looks to add a new block in transactions to the blockchain.**

- **Transactions: A transaction refers to a contract or agreement and transfers of assets between parties. The asset is typically cash or property. The network of computers in blockchain stores the transactional data as copy with the storage typically referred to as a digital ledger.**

- **Block: A block in a blockchain network is similar to a link in a chain. In the field of cryptocurrency, blocks are like records that store transactions like a record book, and those are encrypted into a hash tree.**

- **Chain: Chain is the concept where all the blocks are connected with the help of a chain in the whole blockchain structure in the world. And those blocks are connected with the help of the previous block hash and it indicates a chaining structure.**

- **Miners: Blockchain mining is a process that validates every step in the transactions while operating all cryptocurrencies. People involved in this mining they called miners. Blockchain mining is a process to validate each step in the transactions while operating cryptocurrencies.**

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

2. a) Discuss about the advantages and disadvantages of blockchain.

Ans 2. a)

Advantages of Blockchain Technology:

1. **Open: One of the major advantages of blockchain technology is that it is accessible to all means anyone can become a participant in the contribution to blockchain technology, one does not require any permission from anybody to join the distributed network.**
2. **Verifiable: Blockchain technology is used to store information in a decentralized manner so everyone can verify the correctness of the information by using zero-knowledge proof through which one party proves the correctness of data to another party without revealing anything about data.**
3. **Permanent: Records or information which is stored using blockchain technology is permanent means one needs not worry about losing the data because duplicate copies are stored at each local node as it is a decentralized network that has a number of trustworthy nodes.**
4. **Free from Censorship: Blockchain technology is considered free from censorship as it does not have control of any single party rather it has the concept of trustworthy nodes for validation and consensus protocols that approve transactions by using smart contracts.**
5. **Tighter Security: Blockchain uses hashing techniques to store each transaction on a block that is connected to each other so it has tighter security. It uses SHA 256 hashing technique for storing transactions.**
6. **Immutability: Data cannot be tampered with in blockchain technology due to its decentralized structure so any change will be reflected in all the nodes so one cannot do fraud here, hence it can be claimed that transactions are tamper-proof.**
7. **Transparency: It makes histories of transactions transparent everywhere all the nodes in the network have a copy of the transaction in the network. If any changes occur in the transaction it is visible to the other nodes.**
8. **Efficiency: Blockchain removes any third-party intervention between transactions and removes the mistake making the system efficient and faster. Settlement is made easier and smooth.**
9. **Cost Reduction: As blockchain needs no third man it reduces the cost for the businesses and gives trust to the other partner.**

Disadvantages of Blockchain Technology:

1. **Scalability: It is one of the biggest drawbacks of blockchain technology as it cannot be scaled due to the fixed size of the block for storing information. The block size is 1 MB due to which it can hold only a couple of transactions on a single block.**

2. **Immaturity: Blockchain is only a couple-year-old technology so people do not have much confidence in it, they are not ready to invest in it yet several applications of blockchain are doing great in different industries but still it needs to win the confidence of even more people to be recognized for its complete utilization.**

3. **Energy Consuming: For verifying any transaction a lot of energy is used so it becomes a problem according to the survey it is considered that 0.3 percent of the world's electricity had been used by 2018 in the verification of transactions done using blockchain technology.**

4. **Time-Consuming: To add the next block in the chain miners need to compute nonce values many times so this is a time-consuming process and needs to be speed up to be used for industrial purposes.**

5. **Legal Formalities: In some countries, the use of blockchain technology applications is banned like cryptocurrency due to some environmental issues they are not promoting to use blockchain technology in the commercial sector.**

6. **Storage: Blockchain databases are stored on all the nodes of the network creates an issue with the storage, increasing number of transactions will require more storage.**

7. **Regulations: Blockchain faces challenges with some financial institution. Other aspects of technology will be required in order to adopt blockchain in wider aspect.**

2. b) Enlist and explain the applications of blockchain in detail.

Ans 2. b)

Applications of Blockchain are as follows:

1. Bitcoin: The primary application of Blockchain is in Cryptocurrencies like Bitcoin. Bitcoin is a decentralized digital currency introduced by Santoshi Nakamoto.

2. Banking: Nowadays, Blockchain is also replacing the existing, or we can say overtaking the current Banking system. With the help of Blockchain, we can transfer the fund from one person to another in a second because the transaction's validation will take place through Blockchain and cryptography. It's a possibility that Blockchain will cut down 19.8 Billion Dollars which is going for middleman cost/year. Because of the Blockchain, the hacking of accounts will become impossible.

3. Payment and Transfers: Because of Blockchain, only the wallet system has grown up so rapidly, and by using that, we can make the payment and money transfers very quickly; we don't need to enter the public key. We need to scan a unique QR code and pay soon. The amount done by Blockchain will be highly secure with no transfer fees. For blockchain transfer, no bank account is needed. 4. Healthcare: Healthcare is also a domain where Blockchain technology has been used for storing the details of the patients. This technology ensures that anyone accessing this Blockchain can access patients' data. This database will be highly secure and for checking the data related to the patient-doctor has to log in there with the public key and details, and he can check the patients' data.

5. Law Enforcement: The law enforcement agency is also now applying applications of Blockchain technology. So that they can create a Common Database of the criminal and the crimes committed by them with all the biometric details. Since it's highly secure, nobody can change it without proper access.

6. Voting: Blockchain can be used in the next election or Voting because of its unchanging revolutionary nature. Voting will become more secure and fail-proof with the help of Blockchain.

3. a) Differentiate between Public and Private Ledgers.

Ans 3. a)

S.no	Basis of Comparison	Public BlockChain	Private BlockChain
1.	Access	In this type of blockchain anyone can read, write and participate in a blockchain. Hence, it is permissionless blockchain. It is public to everyone.	In this type of blockchain read and write is done upon invitation, hence it is a permissioned blockchain.
2.	Network Actors	Don't know each other	Know each other
3.	Decentralized Vs Centralized	A public blockchain is decentralized.	A private blockchain is more centralized.
4.	Order Of Magnitude	The order of magnitude of a public blockchain is lesser than that of a private blockchain as it is lighter and provides transactional throughput.	The order of magnitude is more as compared to the public blockchain.
5.	Native Token	Yes	Not necessary
6.	Speed	Slow	Fast
7.	Transactions per second	Transactions per second are lesser in a public blockchain.	Transaction per second is more as compared to public blockchain.
8.	Security	A public network is more secure due to decentralization and active participation. Due to the higher number of nodes in the network, it is nearly impossible for 'bad actors' to attack the system and gain control over the consensus network.	A private blockchain is more prone to hacks, risks, and data breaches/ manipulation. It is easy for bad actors to endanger the entire network. Hence, it is less secure.

9.	Energy Consumption	A public blockchain consumes more energy than a private blockchain as it requires a significant amount of electrical resources to function and achieve network consensus.	Private blockchains consume a lot less energy and power.
10.	Consensus algorithms	Some are proof of work, proof of stake, proof of burn, proof of space etc.	Proof of Elapsed Time (PoET), Raft, and Istanbul BFT can be used only in case of private blockchains.
11.	Attacks	In a public blockchain, no one knows who each validator is and this increases the risk of potential collision or a 51% attack (a group of miners which control more than 50% of the network's computing power.).	In a private blockchain, there is no chance of minor collision. Each validator is known and they have the suitable credentials to be a part of the network.
12.	Effects	Potential to disrupt current business models through disintermediation. There is lower infrastructure cost. No need to maintain servers or system admins radically. Hence reducing the cost of creating and running decentralized application (dApps).	Reduces transaction cost and data redundancies and replace legacy systems, simplifying documents handling and getting rid of semi manual compliance mechanisms.
13.	Examples	Bitcoin, Ethereum, Monero, Zcash, Dash, Litecoin, Stellar, Steemit etc.	R3 (Banks), EWF (Energy), B3i (Insurance), Corda.

3. b) What do you understand by the term Hyperledger? Draw and explain its framework.

Ans 3. b)

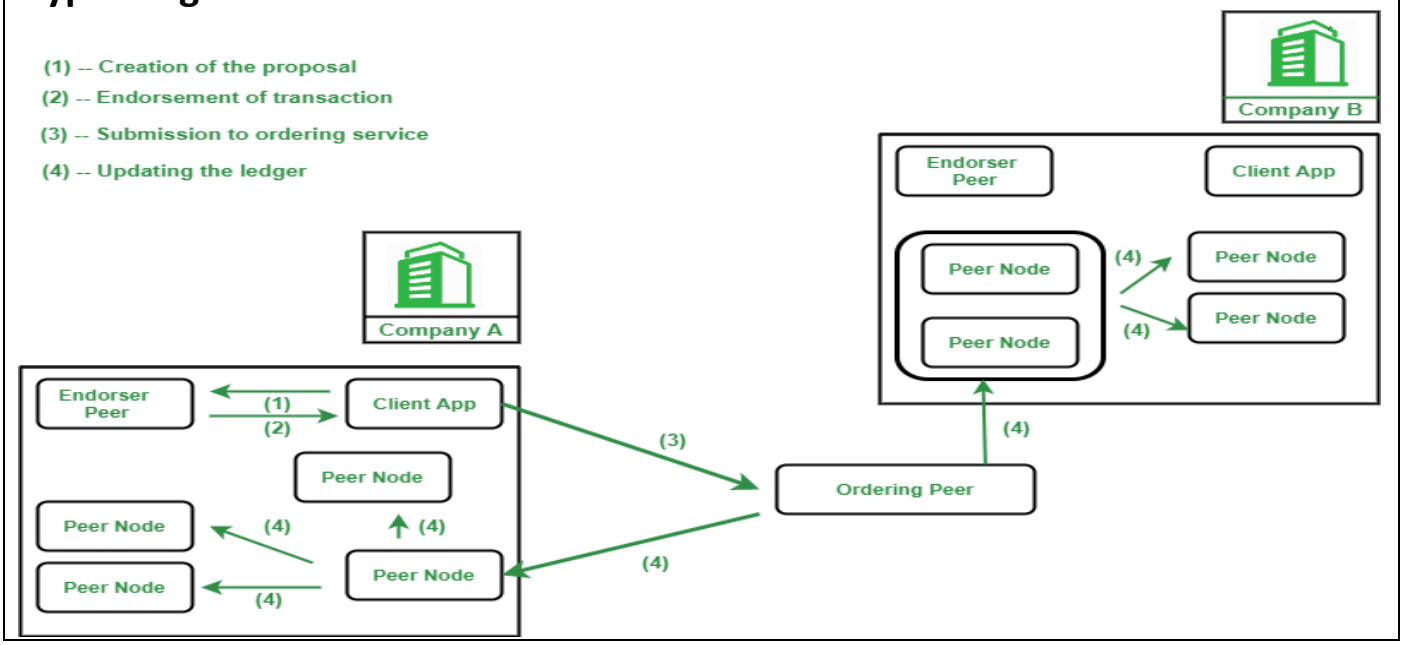
- **Hyperledger is an open source project created to support the development of blockchain-based distributed ledgers. Hyperledger consists of a collaborative effort to create the needed frameworks, standards, tools and libraries to build blockchains and related applications.**

- **Since Hyperledger's creation by the Linux Foundation in 2016, the project has had contributions from organizations such as IBM and Intel, Samsung, Microsoft, Visa, American Express and blockchain startups such as Blockforce. In all, the collaboration includes banking, supply chain management, internet of things (IoT), manufacturing and production-based fields.**

- **Hyperledger acts as a hub for different distributed ledger frameworks and libraries. With this, a business could use one of Hyperledger's frameworks, for example, to improve the efficiency, performance and transactions in their business processes.**

- **Hyperledger works by providing the needed infrastructure and standards for developing blockchain systems and applications. Developers use Hyperledger Greenhouse (the frameworks and tools that make up Hyperledger) to develop business blockchain projects. Network participants are all known to each other and can participate in consensus-making processes.**

Hyperledger Framework



Hyperledger Framework Workflow:
For each and every transaction in the fabric, the following steps are followed-

1. **Creation of the proposal: Imagine a deal between a smartphone manufacturer company and a smartphone dealership. The transaction begins when a member organization proposes or invokes a transaction request with the help of the client application or portal. Then the client application sends the proposal to peers in each organization for endorsement.**

2. **Endorsement of the transaction: After the proposal reaches the endorser peers (peers in each organization for endorsement of a proposal) the peer checks the fabric certificate authority of the requesting member and other details that are needed to authenticate the transaction. Then it executes the chain code (a piece of code that is written in one of the supported languages such as Go or Java) and returns a response. This response indicates the approval or rejection of the following transaction. The response is carried out to the client.**

3. **Submission to ordering service: After receiving the endorsement output, the approved transactions are sent to the ordering service by the client-side application. The peer responsible for the ordering service includes the transaction into a specific block and sends it to the peer nodes of different members of the network.**

4. **Updating the ledger: After receiving this block the peer nodes of such organizations update their local ledger with this block. Hence the new transactions are now committed.**

4. a) Explain the use of Cryptography in Cryptocurrencies.

Ans 4. a)

4. b) Describe cryptographic algorithm - SHA 256.

Ans 4. b)

5. a) Discuss in brief about Hardness of Bitcoin Mining.

Ans 5. a)

Hardness of Bitcoin Mining

- **In order to ensure bitcoin blocks are discovered roughly every 10 minutes, an automatic system is in place that adjusts the difficulty depending on how many miners are competing to discover blocks at any given time.**

- **As the name implies, bitcoin mining difficulty refers to the degree of difficulty involved in discovering new bitcoin blocks through mining.**

- **Because the Bitcoin network is completely decentralized and not run by any single overarching authority, an algorithm hard-coded into the source code by Bitcoin's creator(s) Satoshi Nakamoto is used.**

- **This algorithm constantly readjusts the difficulty of the mining process in line with how many miners are operating in the network to ensure that blocks are discovered at a steady pace.**

5. b) How does Double Spending Happen? What are its type?

Ans 5. b)

How Does Double Spending Happen?

Double spending can never arise physically. It can happen in online transactions. This mostly occurs when there is no authority to verify the transaction. It can also happen if the user's wallet is not secured.

- **Suppose a user wants to avail of services from Merchant 'A' and Merchant 'B'.**
- **The user first made a digital transaction with Merchant 'A'.**
- **The copy of the cryptocurrency is stored on the user's computer.**
- **So, the user uses the same cryptocurrency to pay Merchant 'B'**
- **Now both the merchants have the illusion that the money has been credited since the transactions were not confirmed by the miners.**
- **This is the case of double spending.**

Types Of Double Spending Attacks

There are different types of Double Spending attacks:

- **Finney Attack: Finney Attack is a type of Double spending Attack. In this, a merchant accepts an unauthorized transaction. The original block is eclipsed by the hacker using an eclipse attack. The transaction is performed on an unauthorized one. After that, the real block shows up and again the transaction is done automatically for the real block. Thus the merchant loses money two times.**

- **Race attack: is an attack in which there is a 'race' between two transactions. The attacker sends the same money using different machines to two different merchants. The merchants send their goods but transactions get invalid.**

- **51% Attack: This type of attack is prevalent in small blockchains. Hackers usually take over 51% of the mining power of blockchain and therefore can do anything of their own will.**

6. a) What do you understand by Bitcoin Wallet? Discuss different types.

Ans 6. a)

Bitcoin Wallet

- **A Bitcoin wallet is a digital wallet that can hold Bitcoin as well as other cryptocurrencies, like Ethereum or XRP.**

- **A Bitcoin wallet (and any crypto wallet, for that matter) is a digital wallet storing the encryption material giving access to a Bitcoin public address and enabling transactions**

- **Bitcoin wallets not only hold your digital coins, but they also secure them with a unique private key that ensures that only you, and anyone you give the code to, can open your Bitcoin wallet. Think of it like a password on an online bank account.**

- **With a crypto wallet, you can store, send and receive different coins and tokens. Some just support basic transactions while others include additional features, like built-in access to blockchain-based decentralized applications commonly known as dapps.**

- **Among other things, these may allow you to loan out your cryptocurrency to earn interest on your holdings.**

Types of Bitcoin Wallets

As with physical wallets, Bitcoin wallets come in a range of styles, each offering a tradeoff between convenient access and security against theft.

1. **Mobile**
   Mobile wallets, like WazirX multi-cryptocurrency wallet and Exodus bitcoin wallet are those that run as apps on phones, tablets and other mobile devices.

2. **Web**
   Web-based wallets, like Guarda Bitcoin Wallet, store your coins through an online third party. You can gain access to your coins and make transactions through any device that lets you connect to the internet. These web-based wallets are frequently associated with crypto exchanges that allow you to trade and store crypto all in one place.

While convenient, web-based wallets still hold many of the same risks as mobile wallets, namely that because they're connected to the internet, they can be hacked.

In addition, there have been times when exchanges have shut down, and people lost the coins in their web wallets.

3. **Desktop**
   Desktop wallets, like Guarda and Exodus, are programs you can download onto a computer to store coins on your hard drive. This adds an extra layer of security versus web and mobile apps because you aren't relying on third-party services to hold your coins. Still, hacks are possible because your computer is connected to the internet.

4. **Hardware**
   Hardware wallets are physical devices, like a USB drive, that are not connected to the web. These include Ledger Nano X Bitcoin Wallet and Trezor Model T Bitcoin Wallet available in India.

   To make transactions, you first need to connect the hardware wallet to the internet, either through the wallet itself or through another device with internet connectivity.

   There is typically another password involved to make the connection, which increases security but also raises the risk you may lock yourself out of your crypto if you lose the password.

   Hardware-based crypto wallets are also known as cold storage or cold wallets. (Wallets connected to the internet, in contrast, are called "hot wallets.")

5. **Paper Wallets**
   In a paper wallet, you print off your key, typically a QR code, on a paper document. This makes it impossible for a hacker to access and steal the password online, but then you need to protect the physical document.

6. b) Write short notes on POW and POS.

Ans 6. b)

Proof of Work (PoW)

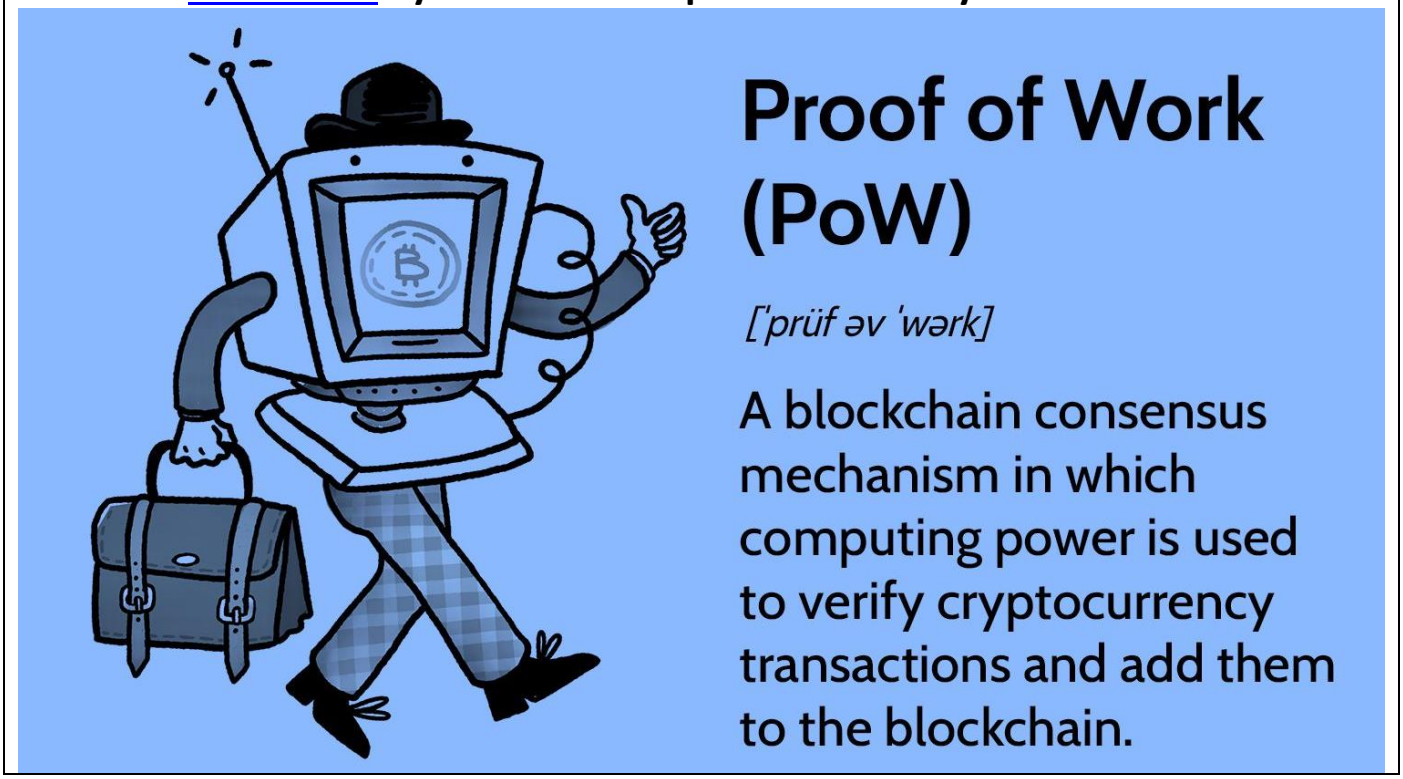
- **Proof of Work consensus is the mechanism of choice for the majority of cryptocurrencies currently in circulation. The algorithm is used to verify the transaction and create a new block in the blockchain.**

- **Proof of Work(PoW) is the original consensus algorithm in a blockchain network. The algorithm is used to confirm the transaction and creates a new block to the chain. In this algorithm, minors (a group of people) compete against each other to complete the transaction on the network.**

- **The process of competing against each other is called mining. As soon as miners successfully created a valid block, he gets rewarded. The most famous application of Proof of Work(PoW) is Bitcoin.**

- **Producing proof of work can be a random process with low probability. In this, a lot of trial and error is required before a valid proof of work is generated.**

- **The main working principle of proof of work is a mathematical puzzle which can easily prove the solution. Proof of work can be implemented in a blockchain by the Hashcash proof of work system.**



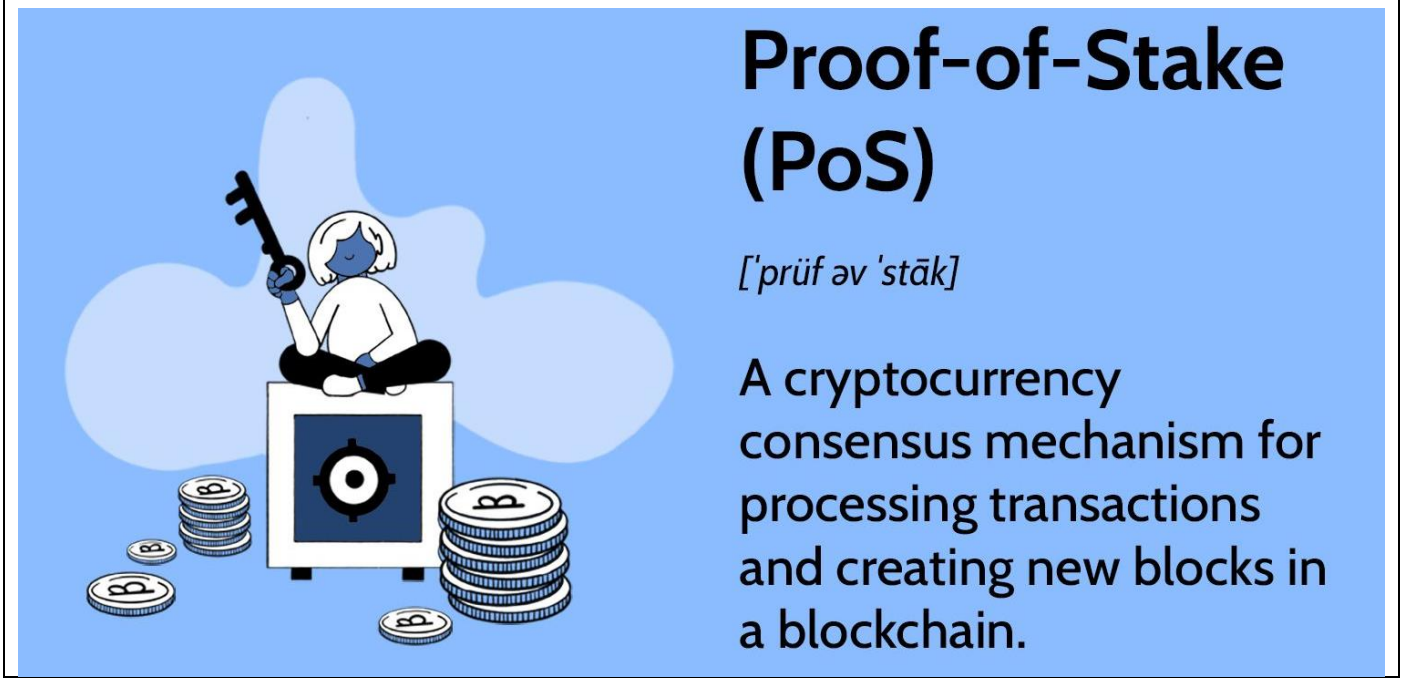
Proof of Stake (PoS)

- **Proof of Stake (PoS) is a type of algorithm which aims to achieve distributed consensus in a Blockchain.**

- **A stake is value/money we bet on a certain outcome. The process is called staking.**

- **Why Proof-of-Stake:**
  - **Before proof of stake, the most popular way to achieve distributed consensus was through Proof-of-Work (implemented in Bitcoin). But Proof-of-Work is quite energy intensive. So, a proof-of-work based consensus mechanism increases an entity's chances of mining a new block if it has more computation resources.**
  - **Apart from the upper two points, there are other weaknesses of a PoW based consensus mechanism which we will discuss later on. In such a scenario, a Proof-of-Stake based mechanism holds merit.**

- **What is Proof-of-Stake:**
  - **As understandable from the name, nodes on a network stake an amount of cryptocurrency to become candidates to validate the new block and earn the fee from it.**
  - **Then, an algorithm chooses from the pool of candidates the node which will validate the new block. This selection algorithm combines the quantity of stake (amount of cryptocurrency) with other factors to make the selection fair to everyone on the network.**



7. a) What do you understand by Ethereum Virtual Machine (EVM)? How Does EVM Works?

Ans 7. a)

Ethereum Virtual Machine (EVM)

- **Ethereum Virtual Machine (EVM) is designed as the runtime environment for smart contracts in Ethereum.**
- **It is sandboxed and isolated from the other parts of the system.**
- **This means that any operation on EVM should not affect your data or programs in any way, no matter how many times you call a particular function on it.**
- **An EVM is the runtime environment that executes Ethereum smart contracts.**
- **Ethereum contains its own Turing-complete scripting language, called Solidity, and with this comes a need to execute this code.**
- **A program called the Ethereum Virtual Machine (EVM) can do this task.**
- **It runs on top of the Ethereum network, meaning that all nodes reach a consensus about what code should be executed at every given time.**
- **To simply explain a Ethereum virtual machine; it is a software platform; which is more like a virtual computer that is used by developers in order to create decentralized applications or DApps.**
- **Developers can also use the EVMs to execute and deploy smart contracts on the Ethereum network.**
- **If one is a programmer with an interest in DApps or if an investor is looking to learn more about the ever-evolving world of EVM crypto, the most probable or the most important term that they would probably have heard of would be Ethereum virtual machines.**

- **To simply explain a Ethereum virtual machine; it is a software platform; which is more like a virtual computer that is used by developers in order to create decentralized applications.**

- **Developers can also use the EVMs to execute and deploy smart contracts on the Ethereum network. If one is a programmer with an interest or if an investor is looking to learn more about the ever-evolving world of EVM crypto, the most probable or the most important term that they would probably have heard of would be Ethereum virtual machines.**

- **According to the creator of the second largest crypto according to market cap, Ethereum, Vitalik Buterin, the main purpose of Ethereum virtual machine is to dictate the state of every block in the Ethereum blockchain.**

Working of EVM

- **To understand it better; EVMs works similar to how other blockchain-based networks.**

- **It is so because they also use a distributed ledger in order to maintain databases for transactions.**

- **Along with that, EVMs also add another layer of functioning because of their smart contract capabilities.**

7. b) Discuss about pros and cons in case of EVM.

Ans 7. b)

Pros of EVM

There are certain benefits of the Ethereum Virtual Machine. They are:

- **Anyone can create their decentralised application via EVM as it has no involvement of security obstacles.**

- **Nowadays, NFTs or Non-Fungible Tokens, are gaining a lot of fame in cryptocurrency. With adequate knowledge about these financial securities, you can create digital art and sell it on a decentralised market using EVMs.**

Cons of EVM

Unlike advantages, there are some disadvantages of the Ethereum virtual machine. Let's see them too:

- **If the owners of these services discontinue using Ethereum, the nodes will stop doing any function, thereby crumbling the entire network.**

- **Using an EVM requires certain technical proficiency. Hence, it is limited to those who do not know to code. Only a few applications have Graphical User Interfaces (GUIs) that only enable some selected individuals to gain the advantage of NFTs.**

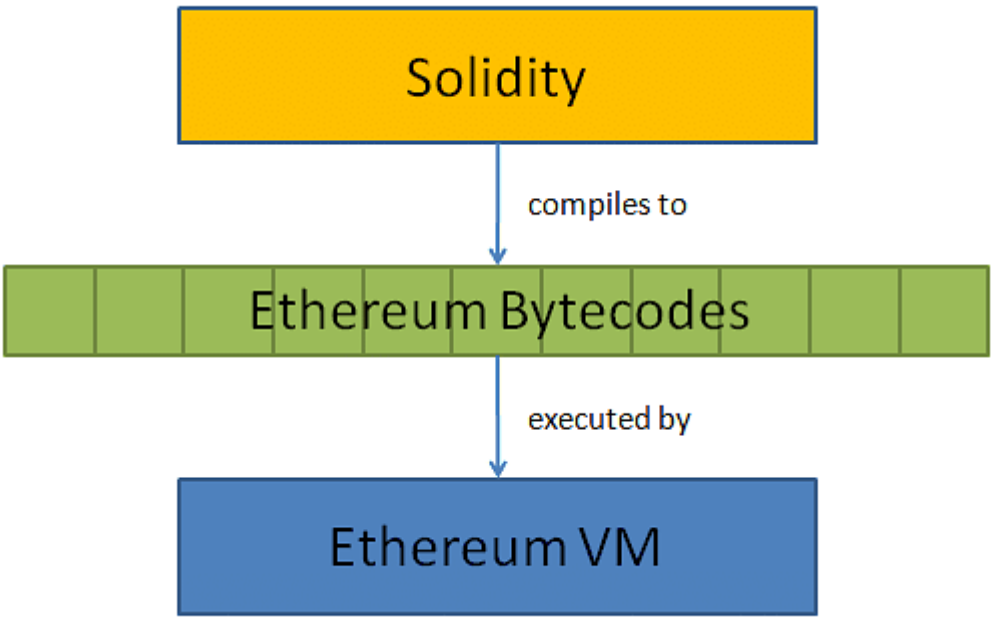
Ethereum is also called a 'global/world computer' as all Ethereum network nodes successfully run the EVM and implement similar instructions. It makes all other nodes reach a consensus about the system's state.

8. a) Write short notes on Ethereum Solidity.

Ans 8. a)

Ethereum Solidity

- **Solidity is a brand-new programming language developed by Ethereum, the second-largest cryptocurrency market by capitalization.**
- **Solidity is an object-oriented programming language created specifically by the Ethereum Network team for constructing and designing smart contracts on Blockchain platforms.**
- **It's used to create smart contracts that implement business logic and generate a chain of transaction records in the blockchain system.**
- **It acts as a tool for creating machine-level code and compiling it on the Ethereum Virtual Machine (EVM).**
- **It has a lot of similarities with C and C++ and is pretty simple to learn and understand. For example, a "main" in C is equivalent to a "contract" in Solidity.**
- **Like other programming languages, Solidity programming also has variables, functions, classes, arithmetic operations, string manipulation, and many other concepts.**
- **Solidity is a relatively new language that is rapidly growing.**
- **Solidity is currently the core language on Ethereum and other private blockchains operating on competing platforms, such as Monax and its Hyperledger Burrow blockchain which uses Tendermint for consensus.**
- **SWIFT has created a proof of concept that runs on Burrow and uses Solidity.**



8. b) What are smart contracts on blockchain?

Ans 8. b)

Smart Contracts on Blockchain

Smart contracts are computer programs or protocols for automated transactions that are stored on a blockchain and run in response to meeting certain conditions. In other words, smart contracts automate the execution of agreements so that all participants can ascertain the outcome as soon as possible without the involvement of an intermediary or time delay.

- **Smart contracts are self-executing contracts in which the contents of the buyer-seller agreement are inscribed directly into lines of code.**
- **According to Nick Szabo, an American computer scientist who devised a virtual currency called "Bit Gold" in 1998, Smart contracts are computerized transaction protocols that execute contract conditions.**
- **Using it makes the transactions traceable, transparent, and irreversible.**

Benefits of Smart Contracts

➢ **Accuracy, Speed, and Efficiency**
- **The contract is immediately executed when a condition is met.**
- **Because smart contracts are digital and automated, there is no paperwork to deal with, and**
- **No time was spent correcting errors that can occur when filling out documentation by hand.**

➢ **Trust and Transparency**
- **There's no need to worry about information being tampered with for personal gain because there's no third party engaged and**
- **Encrypted transaction logs are exchanged among participants.**

➢ **Security**
- **Because blockchain transaction records are encrypted, they are extremely difficult to hack.**
- **Furthermore, because each entry on a distributed ledger is linked to the entries before and after it, hackers would have to change the entire chain to change a single record.**

➢ **Savings**
- **Smart contracts eliminate the need for intermediaries to conduct transactions, as well as the time delays and fees that come with them.**

9. a) Discuss about different Blockchain Implementation Challenges.

Ans 9. a)

Blockchain Implementation Challenges

1. **Lack of adoption**

- Blockchains function more effectively and efficiently when used across a wide network of users. A blockchain ecosystem, for example, would not only need users to join the network but also its suppliers. APQC, on the other hand, has discovered that just 29% of organizations are experimenting with or fully utilizing blockchain. Without broad adoption, blockchains will remain ineffective and scalable.
- However, there are some indications that blockchain adoption will continue to spread. Businesses are gradually coming together and forming collaborative blockchain working groups to tackle similar problems and provide solutions that may benefit everyone without giving away proprietary information.

2. **The rising cost of blockchain implementation**

- It's all about early financial outlays. For some companies, implementation expenditures may be prohibitive. Even if most current solutions are free, a significant investment is required when hiring skilled software engineers who specialize in blockchain development, licensing fees in case of switching to a chargeable software version, overall administration, and more.
- It is one of the most important blockchain implementation challenges.
- If businesses aren't prepared to devote a significant amount of money, perhaps it's better to put off the blockchain introduction.

3. **Scalability**

- The main difficulty with its implementation is scalability. Though transaction networks can handle hundreds of transactions per second without failure, when it comes to Bitcoin (roughly 3-7 transactions per second) and Ethereum (about 15-20 transactions), processing the transactions slows down considerably, making blockchain unviable for large-scale apps.
- Lightning Network and Plasma for Ethereum are scaling technologies that allow fast, low-fee transactions. For widespread adoption to take place, blockchain must improve its speed.

4. **Security and privacy challenges**

- What are some of the most pressing questions you should consider? What about the numerous security and privacy concerns? While cryptocurrencies provide pseudonymity, many potential blockchain applications need smart transactions and contracts to be indisputably linked to real identities, raising significant privacy and data security issues.
- Many businesses today operate under the constraints of legislation. Their customers put their trust in them with important information. However, if all of this data is kept on a public ledger, it will not be truly private. Private or consortia blockchain technology may be utilized here. You would only have enough access, and your confidential information would remain secure.

5. **Regulations**

- The lack of regulation will be the next area where you may face difficulties. Scams and market manipulation that might trigger a global economic collapse are not out of the question. As a result, Bitcoin has been getting lots of negative attention from all around the world.
- Some countries have outright banned bitcoin, while others attempt to regulate blockchain networks with little success.

6. **Criminal activities**

- The absence of stringent legislation and the fact that blockchain is still a developing technology have fueled the rise of fraudulent projects and other bad actors seeking to profit from inexperienced investors. There have also been several high-profile cryptocurrency exchange thefts, including Mt. Gox's infamous bitcoin theft in 2014, nearly destroying the entire cryptocurrency industry.

7. **Energy consumption**

- Another worry is that Proof of Work, the most widely used consensus algorithm, is energy intensive. This restricts entry for regular people into PoW networks, encourages the formation of big mining pools, and prevents decentralization by pushing individuals to join large mining pools, and it also raises environmental concerns.

8. **51% attacks**

- The architecture of blockchain technologies is distinct. Some are more secure than others. The decentralized blockchains, for example, are more vulnerable to 51% attacks than the centralized ones. This has

introduced a few issues for crypto investors who want to store their assets on decentralized chains.

- 51% attacks, in which hackers acquire more than half of the network's computational power, are an issue that has plagued many blockchain systems. They exploit an inherent loophole in decentralized systems, allowing users to control a chain by controlling over 51% of the processing power. This typically happens on networks that use the proof-of-work (PoW) framework.

9. Low workforce availability

- Over the last year, the nonfungible token (NFT) and DeFi industries have seen a tremendous rise in nonfungible tokens and projects, leading to labor market issues. According to recent data, demand for blockchain talent has increased by over 300% among both established businesses and startups as they look for top-tier personnel.
- The scarcity of experienced developers in the blockchain industry has worsened due to high competition between firms offering highly competitive compensation packages to attract and retain their employees. As a result, some businesses in the crypto sector are paying more than $1 million per year to workers in specific job categories. Businesses are calling coders to fill the blockchain talent gap. One of the blockchain implementation challenges is getting the closest to being solved day by day.

10. Interoperability

- One of the most important issues that must be addressed is interoperability, as this is one of the primary reasons businesses are yet hesitant to embrace blockchain technology. Most blockchains are maintained in isolation and do not communicate with other peer networks since they cannot transmit and receive data from a different blockchain-based system.
- They grant access to all of the data in a wallet once generated. It jeopardizes both confidential information and money if stolen. Wallet access is lost for good if lost or destroyed. It is one of the most dangerous blockchain implementation challenges.

9. b) Explain about Zero Knowledge proofs and protocols in Blockchain.

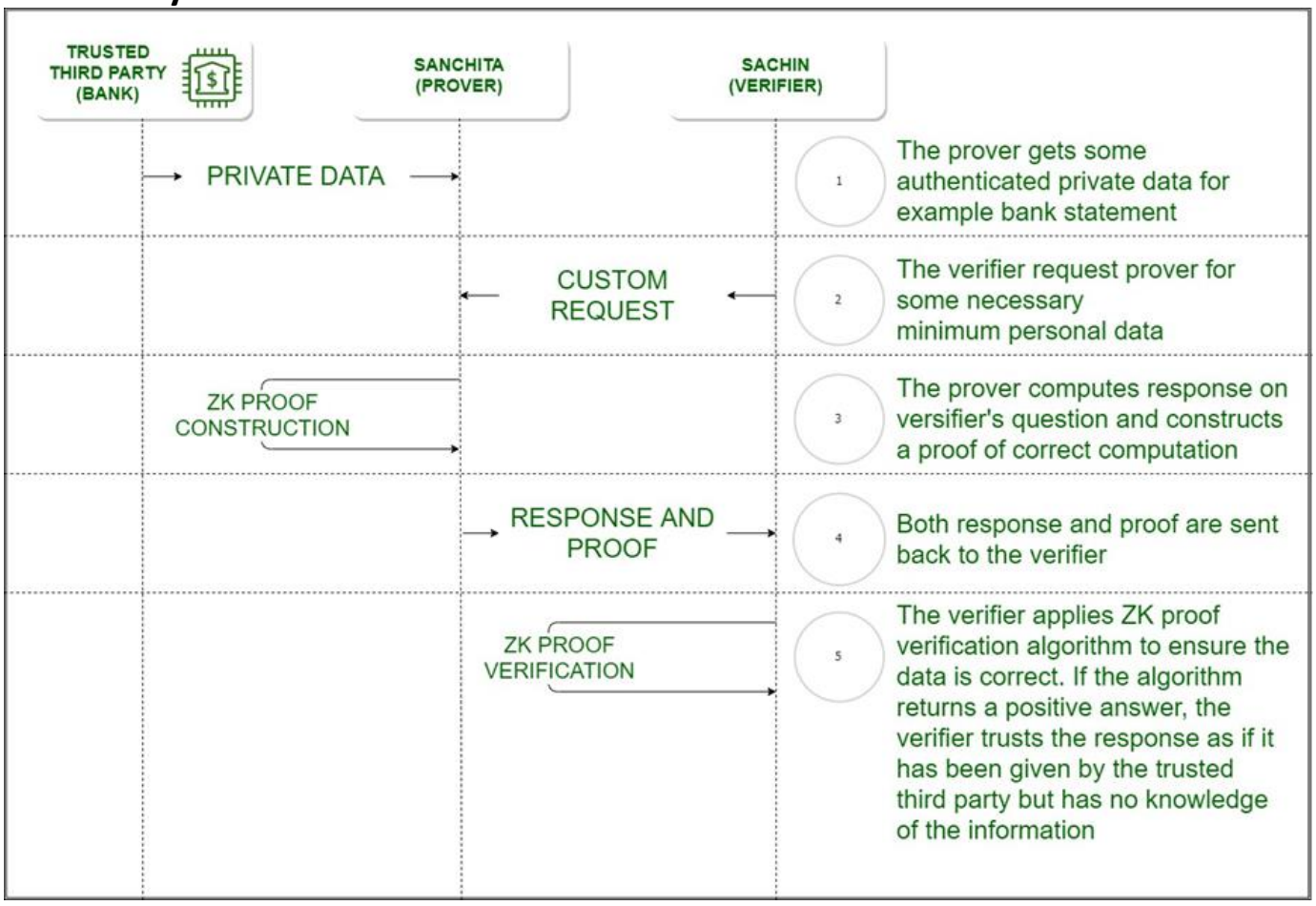
Ans 9. b)

Zero Knowledge Proof

- **Zero Knowledge Proof (ZKP) is an encryption scheme originally proposed by MIT researchers Shafi Goldwasser, Silvio Micali and Charles Rackoff in the 1980s.**

- **Zero-knowledge protocols are probabilistic assessments, which means they don't prove something with as much certainty as simply revealing the entire information would. They provide unlinkable information that can together show the validity of the assertion is probable.**

- **Currently, a website takes the user password as an input and then compares its hash to the stored hash. Similarly a bank requires your credit score to provide you the loan leaving your privacy and information leak risk at the mercy of the host servers. If ZKP can be utilized, the client's password is unknown the to verifier and the login can still be authenticated. Before ZKP, we always questioned the legitimacy of the prover or the soundness of the proof system, but ZKP questions the morality of the verifier. What if the verifier tries to leak the information?**



Example-1: A Colour-blind friend and Two balls :

There are two friends Sachin and Sanchita, out of whom Sanchita is colour blind. Sachin has two balls and he needs to prove that both the balls our of different colour. Sanchita switches the balls randomly behind her back and shows it to Sachin who has to tell if the balls are switched or not. If the balls are of the same colour and Sachin had given false information, the probability of him answering correctly is 50%. When the activity is repeated several times, the probability of Sachin giving the correct answer with the false information is significantly low. Here Sachin is the "prover" and Sanchita is the "verifier". Colour is the absolute information or the algorithm to be executed, and it is proved of its soundness without revealing the information that is the colour to the verifier.

Example-2: Finding Waldo :

Finding Waldo is a game where you have to find a person called Waldo from a snapshot of a huge crowd taken from above. Sachin has an algorithm to find Waldo but he doesn't want to reveal it to Sanchita. Sanchita wants to buy the algorithm but would need to check if the algorithm is working. Sachin cuts a small hole on a cardboard and places over Waldo. Sachin is the "prover" and Sanchita is the "verifier". The algorithm is proved with zero knowledge about it.

Properties of Zero Knowledge Proof :

- **Zero-Knowledge –**
  If the statement is true, the verifier will not know that the statement or was. Here statement can be an absolute value or an algorithm.

- **Completeness –**
  If the statement is true then an honest verifier can be convinced eventually.

- **Soundness –**
  If the prover is dishonest, they can't convince the verifier of the soundness of the proof. Types of Zero Knowledge Proof :

- **Interactive Zero Knowledge Proof –**
  It requires the verifier to constantly ask a series of questions about the "knowledge" the prover possess. The above example of finding Waldo is interactive since the "prover" did a series of actions to prove the about the soundness of the knowledge to the verifier.

- **Non-Interactive Zero Knowledge Proof –**
  For "interactive" solution to work, both the verifier and the prover needed to be online at the same time making it difficult to scale up on the real world application. Non-interactive Zero-Knowledge Proof do not require an interactive process, avoiding the possibility of collusion. It requires picking a hash function to randomly pick the challenge by the verifier. In 1986, Fiat and Shamir invented the Fiat-Shamir heuristic and successfully changed the interactive zero-knowledge proof to non-interactive zero knowledge proof.

10.) Write notes on:

i) Succinct non interactive argument for Knowledge (SNARK)

ii) Pairing on Elliptic curves

iii) Zcash - attacks on Blockchains

Ans 10.)

i) Succinct non interactive argument for Knowledge (SNARK)

SNARKs in blockchain

- **Even though cryptocurrency transactions aren't tied to anyone's identity, they're normally traceable because they're publicly recorded on a blockchain. If you want to avoid this, you'll need a specific type of cryptocurrency called a privacy coin. One of the methods privacy coins use to keep transactions anonymous is with a technology called zk-SNARKs.**
- **Blockchain crypto technology symbolizing chain of block in digital ledger for cryptocurrency like bitcoin or ethereum. Data security and encryption. Connected nodes, fintech. Abstract background.**
- **For those who are considering privacy coins for personal use or as a cryptocurrency investment, it's important to understand the technology behind them. While zk-SNARKs is somewhat complicated, we'll cover exactly what it does in this guide.**

What is zk-SNARK?

- **A zk-SNARK is a zero-knowledge proof protocol where one can prove they possess certain information without revealing it and without any interaction between the parties proving and verifying the information.**
- **The term "zk-SNARK" is an acronym that stands for "Zero-Knowledge Succinct Non- Interactive Argument of Knowledge." Each part of the name refers to a characteristic of zk- SNARKs, so it helps to look at each component separately:**

Zero-Knowledge:

- **The prover can show the verifier that they have a piece of information without providing the information itself.**
- **Succinct: The proof can be verified within a few milliseconds since the proof length is only a few hundred bytes at most.**
- **Non-Interactive: The proof consists of a single message from the prover to the verifier.**

- **Argument: Argument is the term used for these proofs because they don't quite fit the traditional definition of proofs, but they effectively serve the same purpose.**
- **Knowledge: Knowledge refers to the information possessed by the prover.**
- **In cryptocurrency, zk-SNARKs are a way for transactions to be private and fully encrypted on the blockchain while still being validated using the network's consensus rules. zk-SNARKs can show that the sender has the amount of funds they want to transfer without making that information public.**

How zk-SNARKs work

- **With most types of cryptocurrency, a transaction is validated by the network checking that certain conditions have been met. Specifically, the conditions are that the sender has the funds available and that they've provided the correct private key to show that the funds are theirs.**
- **zk-SNARKs allow the sender of a transaction to prove all that without revealing any of the addresses or amounts involved. To offer this, the blockchain network encodes some of its consensus rules in zk-SNARKs.**
- **During the transaction process, zk-SNARKs turn the information that needs to be proved into equations. These equations can be evaluated and solved without disclosing the information itself.**

Pros and cons of zk-SNARKs

- **The primary benefits of zk-SNARKs are the privacy and efficiency they offer. They shield sensitive information, it takes just milliseconds to verify them, and they don't require extended interaction between the parties involved. All that's needed is one message from the prover to the verifier.**
- **Although zk-SNARKs don't have any glaring drawbacks, if someone has the private key used to set up the protocol, they'd be able to create false proofs and counterfeit funds. Privacy coins that use zk-SNARKs must take steps to ensure no single party has access to that private key.**

zk-SNARK vs. zk-Rollup

- **zk-SNARK is far from the only type of zero-knowledge proof used by cryptocurrencies. Another common technology is the zk-Rollup, a scaling solution to help Ethereum (CRYPTO:ETH) process transactions more efficiently.**
- **A rollup bundles a large group of transactions and validates them off-chain, meaning all the computations are handled off the main Ethereum blockchain. They're then rolled up into a single transaction that's sent to Ethereum's execution layer.**

- **There are different types of rollups available. For example, Optimistic rollups assume transactions are valid until they're proven false. zk-Rollups, on the other hand, instantly verify transactions and generate cryptographic validity proofs. The proofs can be generated using zk-SNARKs or another type of zero-knowledge proof technology, zk-STARKs.**

zk-SNARK examples

- **The most well-known example of zk-SNARKs is their use in shielding cryptocurrency transactions. Zcash is the first widespread application of zk-SNARKs. This privacy coin allows users to choose between private and transparent addresses. When a user chooses a private address, zk-SNARKs shield the transaction data.**
- **Other blockchain projects are also using zk-SNARKs. Ethereum started working on integrating Zcash and zk-SNARKs in 2017. That same year, Zcash partnered with JP Morgan Chase (NYSE:JPM) on building a blockchain-based payment system with zk-STARKs.**
- **While zk-SNARKs are currently used to privatize financial transactions, that's not their only application. In the future, we could see them used to protect people's data during online activity.**

ii) Pairing on Elliptic curves

Elliptic Curve Cryptography

Cryptography is the study of techniques for secure communication in the presence of adversarial behavior. Encryption uses an algorithm to encrypt data and a secret key to decrypt it. There are 2 types of encryption:

Symmetric-key Encryption (secret key encryption): Symmetric-key algorithms are cryptographic algorithms that employ the same cryptographic keys both for plaintext encryption and ciphertext decoding. The keys could be identical, or there could be a simple transition between them.
Asymmetric-key encryption (public key encryption): Asymmetric-key algorithms encrypt and decrypt a message using a pair of related keys (one public key and one private key) and safeguard it from unauthorized access or usage.

Elliptic Curve Cryptography (ECC) is an encryption technology comparable to RSA that enables public-key encryption.
While RSA's security is dependent on huge prime numbers, ECC leverages the mathematical theory of elliptic curves to achieve the same level of security with considerably smaller keys. Victor Miller and Neal Koblitz separately proposed elliptic curve ciphers in the mid-1980s. On a high level, they are analogs of actual public cryptosystems in which modular arithmetic is substituted by elliptic curve operations.

Below are the components of elliptic curve cryptography:

1. ECC keys:

Private key: ECC cryptography's private key creation is as simple as safely producing a random integer in a specific range, making it highly quick. Any integer in the field represents a valid ECC private key.
Public keys: Public keys within ECC are EC points, which are pairs of integer coordinates x, and y that lie on a curve. Because of its unique features, EC points can be compressed to a single coordinate + 1 bit (odd or even). As a result, the compressed public key corresponds to a 256-bit ECC.

2. Generator Point:

ECC cryptosystems establish a special pre-defined EC point called generator point G (base point) for elliptic curves over finite fields, which can generate any other position in its subgroup over the elliptic curve by multiplying G from some integer in the range *0…r+.
The number r is referred to as the "ordering" of the cyclic subgroup.

Elliptic curve subgroups typically contain numerous generator points, but cryptologists carefully select one of them to generate the entire group (or subgroup), and is excellent for performance optimizations in calculations. This is the "G" generator.
Elliptic Curve Cryptography Algorithms
Based on the arithmetic of elliptic curves over finite fields, Elliptic-Curve Cryptography (ECC) provides numerous sets of algorithms:

Digital signature algorithms:

Elliptic Curve Digital Signature Algorithm. (ECDSA): ECDSA, or Elliptic Curve Digital Signature Algorithm, is a more highly complicated public-key cryptography encryption algorithm. Elliptic curve cryptography is a type of public key cryptography that uses the algebraic structure of elliptic curves with finite fields as its foundation. Elliptic curve cryptography is primarily used to generate pseudo-random numbers, digital signatures, and other data.
Edwards-curve Digital Signature Algorithm (EdDSA): The Edwards-curve Digital Signature Algorithm (EdDSA) was proposed as a replacement for the Elliptic Curve Digital Signature Algorithm for performing fast public-key digital signatures (ECDSA). Its primary benefits for embedded devices are higher performance and simple, secure implementations. During a signature, no branch or lookup operations based on the secret values are performed. Many side-channel attacks are foiled by these properties.

Encryption algorithms:

- **Elliptic Curve Integrated Encryption Scheme (ECIES): ECIES is a public-key authenticated encryption scheme that uses a KDF (key-derivation function) to generate a separate Medium Access Control key and symmetric encryption key from the ECDH shared secret. Because the ECIES algorithm incorporates a symmetric cipher, it can encrypt any amount of data. In practice, ECIES is used by standards such as Intelligent Transportation Systems.**

- **EC-based ElGamal Elliptic Curve Cryptography: ElGamal Elliptic Curve Cryptography is the public key cryptography equivalent of ElGamal encryption schemes that employ the Elliptic Curve Discrete Logarithm Problem. ElGamal is an asymmetric encryption algorithm that is used to send messages securely over long distances. Unfortunately, if the encrypted message is short enough, the algorithm is vulnerable to a Meet in the Middle attack.**

Key Agreement algorithm:

- **Elliptic-curve Diffie–Hellman (ECDH): Elliptic-curve Diffie-Hellman (ECDH) is a key agreement protocol that enables two parties to establish a shared secret over an insecure channel, each with an elliptic-curve public-private key pair. This shared secret can be used directly as a key or to generate another key. Following that, the key, or the derived key, can be used to encrypt subsequent communications with a symmetric-key cipher.**
- **Fully Hashed Menezes-Qu-Vanstone(FHMQV): Fully Hashed Menezes-Qu-Vanstone is an authenticated key agreement protocol based on the Diffie-Hellman scheme. MQV, like other authenticated Diffie-Hellman schemes, protects against an active attacker. The protocol can be adapted to work in any finite group, most notably elliptic curve groups, in which it is recognized as elliptic curve MQV (ECMQV).**

Application of Elliptic Curve Cryptography

- **Diffie-Hellman: The basic public-key cryptosystem suggested for secret key sharing Diffie-Hellman protocol. If A (Alice) and B (Bob) initially agree on a given curve, field size, and mathematical type. They then distribute the secret key in the following manner. We can see that all we need to build the Diffie-Hellman protocol is scalar multiplication.**
- **Elliptic Curve Digital Signature Algorithm (ECDSA):**
- **Online application:**
- **Blockchain application:**

iii) Zcash - attacks on Blockchains

Zcash - attacks on Blockchains

- **Zcash, a privacy-focused proof-of-work blockchain, has been undergoing a spam attack.**

- **Analysts say the blockchain has processed a large volume of transactions that aim to disrupt the network. To do this, the attacker misused Zcash's "shielded transactions" meant for privacy.**

- **Here, the attacker has been adding hundreds of output values within shielded transactions that are proving to be very data-intensive. As a result, the blockchain size has grown dramatically, going from 31 GB in mid-June to more than 100 GB currently, according to data from Blockchair.**

- **The situation is placing high demands on the network. While Zcash has not had any downtime, the blockchain's rapidly growing size has led to troubles for nodes' ability to sync with the network. On-chain records indicate that while the situation has persisted for months, it has been brought to public attention only recently.**

- **"At this point, there only seems to be two problems with the spam: it's bloating the chain size, and it's making it harder for wallets to sync," Sean Bowe, an engineer at Zcash's core development firm Electric Coin Company said.**

- **Others pointed out that Zcash doesn't have spam prevention systems in place. A transactor pays a small fee of 0.0001 ZEC (worth a few cents) for shielded transactions with hundreds of output values, Zcash's block explorer shows.**

- **"It's sad to see. There was always a risk of DoS given Zcash's deliberate lack of a fee market," security researcher Ian Miers, who has previously worked at Zcash, noted in a tweet Wednesday. "The proofs are much larger and slower to verify, making the attack worse."**
- **THE DAILY**
- **Stay up to date on the most influential events and analysis happening across the digital asset ecoyste**

- **Enter Email**

- **Also receive our FREE weekly Data & Insights Newsletter**
- **By signing-up you agree to our Terms of Service and Privacy Policy**

- **The motive for this attack has not been determined, but industry commentators have offered varying theories.**

- **Nick Bax, head of research at Convex Labs, speculated that someone is trying to profit off harming the network. He also floated a possible theory that the spam attack is an attempt to "make it harder for people to run nodes" as this can potentially allow them to surveil users' activity on the blockchain.**

- **What are shielded transactions?**
- **Across blockchains that use the UTXO model like Zcash, transactions are validated by linking the sender address, receiver address, and input and output values. But these values can be easily traced on a public blockchain. To enforce transactional privacy, Zcash uses cryptographic proofs called zk-SNARKs to obfuscate the input-output values of transactions.**

- **Zcash transactions that make use of this technique are called shielded transactions and are meant for legitimate usage. However, the lack of a fee market can unintentionally let malicious actors spam the network if they use a large number of output variables. On this point, Solana Labs CEO Anatoly suggested that the project should increase the fees by 100 times for each output aiming to reduce spam.**

- **In August, Zcash researchers proposed a new fee mechanism that aimed to incorporate fees based on transaction size. In such a scenario, fee rates would keep increasing when the network is under extreme usage.**