**BLOCKCHAIN TECHNOLOGY LECTURE NOES**

**Q1. BLOCKCHAIN OR DISTRIBUTED TRUST:**

**Answer: -** Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An *asset* can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

Why blockchain is important: Business runs on information. The faster it’s received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members. A blockchain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.

**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.

1. **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.

1. **Smart contracts**

To speed transactions, a set of rules — called a [smart contract](https://www.ibm.com/topics/smart-contracts) — 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.

How blockchain works

As each transaction occurs, it is recorded as a “block” of data

Those transactions show the movement of an asset that can be tangible (a product) or intangible (intellectual). The data block can record the information of your choice: who, what, when, where, how much and even the condition — such as the temperature of a food shipment.

Each block is connected to the ones before and after it

These blocks form a chain of data as an asset moves from place to place or ownership changes hands. The blocks confirm the exact time and sequence of transactions, and the blocks link securely together to prevent any block from being altered or a block being inserted between two existing blocks.

Transactions are blocked together in an irreversible chain: a blockchain

Each additional block strengthens the verification of the previous block and hence the entire blockchain. This renders the blockchain tamper-evident, delivering the key strength of immutability. This removes the possibility of tampering by a malicious actor — and builds a ledger of transactions you and other network members can trust.

**Q2. Benefits of blockchain**

**Answer: -** What needs to change: Operations often waste effort on duplicate record keeping and third-party validations. Record-keeping systems can be vulnerable to fraud and cyberattacks. Limited transparency can slow data verification. And with the arrival of IoT, transaction volumes have exploded. All of this slows business, drains the bottom line — and means we need a better way. Enter blockchain.

**Greater trust**

With blockchain, as a member of a members-only network, you can rest assured that you are receiving accurate and timely data, and that your confidential blockchain records will be shared only with network members to whom you have specifically granted access.

**Greater security**

Consensus on data accuracy is required from all network members, and all validated transactions are immutable because they are recorded permanently. No one, not even a system administrator, can delete a transaction.

**More efficiencies**

With a distributed ledger that is shared among members of a network, time-wasting record reconciliations are eliminated. And to speed transactions, a set of rules — called a smart contract — can be stored on the blockchain and executed automatically.

**Q3. Types of blockchain networks**

**Answer: -** There are several ways to build a blockchain network. They can be public, private, permissioned or built by a consortium.

**Public blockchain networks**

A public blockchain is one that anyone can join and participate in, such as Bitcoin. Drawbacks might include substantial computational power required, little or no privacy for transactions, and weak security. These are important considerations for enterprise use cases of blockchain.

**Private blockchain networks**

A private blockchain network, similar to a public blockchain network, is a decentralized peer-to-peer network. However, one organization governs the network, controlling who is allowed to participate, execute a consensus protocol and maintain the shared ledger. Depending on the use case, this can significantly boost trust and confidence between participants. A private blockchain can be run behind a corporate firewall and even be hosted on premises.

**Permissioned blockchain networks**

Businesses who set up a private blockchain will generally set up a permissioned blockchain network. It is important to note that public blockchain networks can also be permissioned. This places restrictions on who is allowed to participate in the network and in what transactions. Participants need to obtain an invitation or permission to join.

**Consortium blockchains**

Multiple organizations can share the responsibilities of maintaining a blockchain. These pre-selected organizations determine who may submit transactions or access the data. A consortium blockchain is ideal for business when all participants need to be permissioned and have a shared responsibility for the blockchain.

Blockchain security

Risk management systems for blockchain networks

When building an enterprise blockchain application, it’s important to have a comprehensive security strategy that uses cybersecurity frameworks, assurance services and best practices to reduce risks against attacks and fraud.

**Q4. What is DISTRIBUTED TRUST?**

**Answer: -** Trust is an unstable equilibrium. When two people trust each other, it only takes one of them to have doubts for the other to also start doubting. The result is that the parties descend into a state of mutual mistrust, a sentiment that is much less precariously balanced. It therefore takes energy to retain trust; yet it takes information to facilitate this energy. One of our era’s most violent breaks with established models concerns the source of this energy. France follows a model whereby energy is externalised: it is the nation’s judges, teachers, managers, parents, and so on, who are responsible for driving this energy. In the Anglo-Saxon model, the energy comes from both parties (or from the community, when there are several people involved). When eBay was created, it was not the only online auction and shopping website, but it invented the concept of buyers and sellers rating each other, a scoring feature that can now be found on all community sites such as Airbnb, BlaBlaCar, and so. What eBay understood is that trust could only be created by the community itself and not by the presence of third parties, which in its case would have meant expert auctioneers.

**CURRENCY:**

Currency serves as a means of exchanging commodities and services. Money in the form of paper or coins, issued by a government and accepted at face value, is known as currency.  
  
In bartering, goods and services were exchanged directly for other goods and services. Currency has replaced bartering as the primary means of exchanging goods and services in the modern world.

**CRYPTOCURRENCY:**

Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It’s a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When you transfer cryptocurrency funds, the transactions are recorded in a public ledger. Cryptocurrency is stored in digital wallets.

Cryptocurrency received its name because it uses [encryption](https://www.kaspersky.com/resource-center/definitions/encryption) to verify transactions. This means advanced coding is involved in storing and transmitting cryptocurrency data between wallets and to public ledgers. The aim of encryption is to provide security and safety.

The first cryptocurrency was [Bitcoin](https://www.kaspersky.com/resource-center/definitions/what-is-bitcoin), which was founded in 2009 and remains the best known today. Much of the interest in cryptocurrencies is to trade for profit, with speculators at times driving prices skyward.

**Q 5. How does cryptocurrency work?**

**Answer: -** Cryptocurrencies run on a distributed public ledger called blockchain, a record of all transactions updated and held by currency holders.

Units of cryptocurrency are created through a process called mining, which involves using computer power to solve complicated mathematical problems that generate coins. Users can also buy the currencies from brokers, then store and spend them using cryptographic wallets.

If you own cryptocurrency, you don’t own anything tangible. What you own is a key that allows you to move a record or a unit of measure from one person to another without a trusted third party.

Although Bitcoin has been around since 2009, cryptocurrencies and applications of blockchain technology are still emerging in financial terms, and more uses are expected in the future. Transactions including bonds, stocks, and other financial assets could eventually be traded using the technology.

Cryptocurrency examples

There are thousands of cryptocurrencies. Some of the best known include:

Bitcoin:

Founded in 2009, Bitcoin was the first cryptocurrency and is still the most commonly traded. The currency was developed by Satoshi Nakamoto – widely believed to be a pseudonym for an individual or group of people whose precise identity remains unknown.

Ethereum:

Developed in 2015, Ethereum is a blockchain platform with its own cryptocurrency, called Ether (ETH) or Ethereum. It is the most popular cryptocurrency after Bitcoin.

Litecoin:

This currency is most similar to bitcoin but has moved more quickly to develop new innovations, including faster payments and processes to allow more transactions.

Ripple:

Ripple is a distributed ledger system that was founded in 2012. Ripple can be used to track different kinds of transactions, not just cryptocurrency. The company behind it has worked with various banks and financial institutions.

Non-Bitcoin cryptocurrencies are collectively known as “altcoins” to distinguish them from the original.

**Q. 6 How to buy cryptocurrency.**

**Answer: -** You may be wondering how to buy cryptocurrency safely. There are typically three steps involved. These are:

Step 1: Choosing a platform

The first step is deciding which platform to use. Generally, you can choose between a traditional broker or dedicated cryptocurrency exchange:

* Traditional brokers. These are online brokers who offer ways to buy and sell cryptocurrency, as well as other financial assets like stocks, bonds, and ETFs. These platforms tend to offer lower trading costs but fewer crypto features.
* Cryptocurrency exchanges. There are many cryptocurrency exchanges to choose from, each offering different cryptocurrencies, wallet storage, interest-bearing account options, and more. Many exchanges charge asset-based fees.

When comparing different platforms, consider which cryptocurrencies are on offer, what fees they charge, their security features, storage and withdrawal options, and any educational resources.

Step 2: Funding your account

Once you have chosen your platform, the next step is to fund your account so you can begin trading. Most crypto exchanges allow users to purchase crypto using fiat (i.e., government-issued) currencies such as the US Dollar, the British Pound, or the Euro using their debit or credit cards – although this varies by platform.

Crypto purchases with credit cards are considered risky, and some exchanges don't support them. Some credit card companies don't allow crypto transactions either. This is because cryptocurrencies are highly volatile, and it is not advisable to risk going into debt — or potentially paying high credit card transaction fees — for certain assets.

Some platforms will also accept ACH transfers and wire transfers. The accepted payment methods and time taken for deposits or withdrawals differ per platform. Equally, the time taken for deposits to clear varies by payment method.

An important factor to consider is fees. These include potential deposit and withdrawal transaction fees plus trading fees. Fees will vary by payment method and platform, which is something to research at the outset.

Step 3: Placing an order

You can place an order via your broker's or exchange's web or mobile platform. If you are planning to buy cryptocurrencies, you can do so by selecting "buy," choosing the order type, entering the amount of cryptocurrencies you want to purchase, and confirming the order. The same process applies to "sell" orders.

There are also other ways to invest in crypto. These include payment services like PayPal, Cash App, and Venmo, which allow users to buy, sell, or hold cryptocurrencies. In addition, there are the following investment vehicles:

* Bitcoin trusts: You can buy shares of Bitcoin trusts with a regular brokerage account. These vehicles give retail investors exposure to crypto through the stock market.
* Bitcoin mutual funds: There are Bitcoin ETFs and Bitcoin mutual funds to choose from.
* Blockchain stocks or ETFs: You can also indirectly invest in crypto through blockchain companies that specialize in the technology behind crypto and crypto transactions. Alternatively, you can buy stocks or ETFs of companies that use blockchain technology.

The best option for you will depend on your investment goals and risk appetite.

Q. 6 How to store cryptocurrency.

Answer : - Once you have purchased cryptocurrency, you need to store it safely to protect it from hacks or theft. Usually, cryptocurrency is stored in crypto wallets, which are physical devices or online software used to store the private keys to your cryptocurrencies securely. Some exchanges provide wallet services, making it easy for you to store directly through the platform. However, not all exchanges or brokers automatically provide wallet services for you.

There are different wallet providers to choose from. The terms “hot wallet” and “cold wallet” are used:

* Hot wallet storage: "hot wallets" refer to crypto storage that uses online software to protect the private keys to your assets.
* Cold wallet storage: Unlike hot wallets, cold wallets (also known as hardware wallets) rely on offline electronic devices to securely store your private keys.

Typically, cold wallets tend to charge fees, while hot wallets don't.

**Q 7. What can you buy with cryptocurrency?**

**Answer: -** When it was first launched, Bitcoin was intended to be a medium for daily transactions, making it possible to buy everything from a cup of coffee to a computer or even big-ticket items like real estate. That hasn’t quite materialized and, while the number of institutions accepting cryptocurrencies is growing, large transactions involving it are rare. Even so, it is possible to buy a wide variety of products from e-commerce websites using crypto. Here are some examples:

Technology and e-commerce sites:

Several companies that sell tech products accept crypto on their websites, such as newegg.com, AT&T, and Microsoft. Overstock, an e-commerce platform, was among the first sites to accept Bitcoin. Shopify, Rakuten, and Home Depot also accept it.

Luxury goods:

Some luxury retailers accept crypto as a form of payment. For example, online luxury retailer Bitdials offers Rolex, Patek Philippe, and other high-end watches in return for Bitcoin.

Cars:

Some car dealers – from mass-market brands to high-end luxury dealers – already accept cryptocurrency as payment.

Insurance:

In April 2021, Swiss insurer [AXA announced that it had begun accepting Bitcoin as a mode of payment](https://www.axa.ch/en/ueber-axa/blog/trend/bitcoin-cryptocurrency%20.html) for all its lines of insurance except life insurance (due to regulatory issues). Premier Shield Insurance, which sells home and auto insurance policies in the US, also accepts Bitcoin for premium payments.

If you want to spend cryptocurrency at a retailer that doesn’t accept it directly, you can use a cryptocurrency debit card, such as BitPay in the US.

**Q 8. Cryptocurrency fraud and cryptocurrency scams.**

**Answer: -** Unfortunately, cryptocurrency crime is on the rise. Cryptocurrency scams include:

Fake websites: Bogus sites which feature fake testimonials and crypto jargon promising massive, guaranteed returns, provided you keep investing.

Virtual Ponzi schemes: Cryptocurrency criminals promote non-existent opportunities to invest in digital currencies and create the illusion of huge returns by paying off old investors with new investors’ money. One scam operation, BitClub Network, raised more than $700 million before its perpetrators [were indicted in December 2019](https://www.justice.gov/usao-nj/page/file/1224881/download).

"Celebrity" endorsements: Scammers pose online as billionaires or well-known names who promise to multiply your investment in a virtual currency but instead steal what you send. They may also use messaging apps or chat rooms to start rumours that a famous businessperson is backing a specific cryptocurrency. Once they have encouraged investors to buy and driven up the price, the scammers sell their stake, and the currency reduces in value.

Romance scams: The FBI warns of a trend in [online dating scams](https://www.kaspersky.com/resource-center/threats/beware-online-dating-scams), where tricksters persuade people they meet on dating apps or social media to invest or trade in virtual currencies. The FBI’s Internet Crime Complaint Centre fielded more than 1,800 reports of crypto-focused romance scams in the first seven months of 2021, with losses reaching $133 million.

Otherwise, fraudsters may pose as legitimate virtual currency traders or set up bogus exchanges to trick people into giving them money. Another crypto scam involves fraudulent sales pitches for individual retirement accounts in cryptocurrencies. Then there is straightforward cryptocurrency hacking, where criminals break into the digital wallets where people store their virtual currency to steal it.

**Q.9 Is cryptocurrency safe?**

**Answer: -** Cryptocurrencies are usually built using blockchain technology. Blockchain describes the way transactions are recorded into "blocks" and time stamped. It's a fairly complex, technical process, but the result is a digital ledger of cryptocurrency transactions that's hard for hackers to tamper with.

In addition, transactions require a two-factor authentication process. For instance, you might be asked to enter a username and password to start a transaction. Then, you might have to enter an authentication code sent via text to your personal cell phone.

While securities are in place, that does not mean cryptocurrencies are un-hackable. Several high-dollar hacks have cost cryptocurrency start-ups heavily. Hackers hit Coincheck to the tune of $534 million and BitGrail for $195 million, making them [two of the biggest cryptocurrency hacks of 2018](https://www.investopedia.com/news/largest-cryptocurrency-hacks-so-far-year/).

Unlike government-backed money, the value of virtual currencies is driven entirely by supply and demand. This can create wild swings that produce significant gains for investors or big losses. And cryptocurrency investments are subject to far less regulatory protection than traditional financial products like stocks, bonds, and mutual funds.

Four tips to invest in cryptocurrency safely

According to Consumer Reports, all investments carry risk, but some experts consider cryptocurrency to be one of the riskier investment choices out there. If you are planning to invest in cryptocurrencies, these tips can help you make educated choices.

Research exchanges:

Before you invest, learn about cryptocurrency exchanges. It’s estimated that there are over 500 exchanges to choose from. Do your research, read reviews, and talk with more experienced investors before moving forward.

Know how to store your digital currency:

If you buy cryptocurrency, you have to store it. You can keep it on an exchange or in a digital wallet. While there are different kinds of wallets, each has its benefits, technical requirements, and security. As with exchanges, you should investigate your storage choices before investing.

Diversify your investments:

Diversification is key to any good investment strategy, and this holds true when you are investing in cryptocurrency. Don't put all your money in Bitcoin, for example, just because that's the name you know. There are thousands of options, and it's better to spread your investment across several currencies.

Prepare for volatility:

The cryptocurrency market is highly volatile, so be prepared for ups and downs. You will see dramatic swings in prices. If your investment portfolio or mental wellbeing can't handle that, cryptocurrency might not be a wise choice for you.

Cryptocurrency is all the rage right now, but remember, it is still in its relative infancy and is considered highly speculative. Investing in something new comes with challenges, so be prepared. If you plan to participate, do your research, and invest conservatively to start.

CROWD FUNDING:

The Crowdfunding platform in [block-chain](https://www.geeksforgeeks.org/blockchain-technology-introduction/) makes different possibilities for the startups by raising the funds to create their own digital currency and it is peer-to-peer fund raising model some of the famous crowdfunding cryptocurrencies are coinspace, swarm, judobaby etc. Crowdfunding has offers for creators and other consumers. Anyone can participate in this crowdfunding if they have invented any new [cryptocurrency](https://www.geeksforgeeks.org/what-is-a-cryptocurrency/) (e.g., Ethereum) and also can contribute as much as they want.

**Q10. How does BlockChain support Crowdfunding?**

**Answer: -** There are several areas where block-chain supports and improves crowdfunding, crowdfunding platforms powered by blockchain technology removes the need for intermediate third party.

* Decentralization: Since block-chain is decentralized it doesn’t rely on any other platforms to create funds. for starters, no longer to be obliged to any rules and any project can get visibility and funded if the investors think to invest, eliminates fees which makes crowdfunding less expensive for the creators.
* Access Equity: To provide investors equity or ownership block-chain relies on asset tokenization. For example, a person who plans to create multiple new products with the incoming funds and grant small ownerships stake in the company. This could potentially open whole new world of opportunity.
* Universal Opportunity: Any project using a block-chain-based crowdfunding model can get funded. Any person with an internet connection can contribute projects.
* Flexible Options: Using block-chain as asset tokenization grants creators and entrepreneurs more liberties. usually, asset tokens have their own currency to enable organizations to hire professionals and advertisers.
* Peer-to-Peer: The cryptocurrencies are exchangeable on a peer-to-peer network. This usually help the people for their investment which even generates more interest in the entire process.

**Q11. Explain Extensibility of Blockchain concepts.**

**Answer: -** Blockchain technology was introduced to disrupt the financial sector. Many financial institutes and banks have leveraged blockchain to make transactions secure and remove intermediaries.

But blockchain technology is not only restricted to the finance sector. From automobile to retail, healthcare, manufacturing, and travel, every industry is investing in blockchain to avail its benefits.

The technical concept behind the blockchain is similar to that of a database, but the interaction with that database is entirely different.

For developers willing to learn blockchain development, it is essential to understand how they will write software applications in the future and how different blockchain concepts like consensus, trusted computing, smart contracts, and file storage systems interact with one another in a decentralized environment.

To make you learn how to develop blockchain applications or to implement blockchain development in businesses, we have covered the following ground:

**Understanding the basics of Blockchain Development**

If you are a beginner, you should be familiar with the following terms:

* **Blockchain**  
  The blockchain is an incorruptible chain of blocks where each block contains data of value which is validated by all nodes in the network, not by any central authority. Each block in the chain includes its hash value and that of the previous block which acts as a unique fingerprint so that no one can tamper with data stored in it.The information stored on the blockchain can never be deleted or altered. Instead, a new block needs to be added to the chain to update the information.
* **Decentralized**  
  A blockchain is said to be decentralized as it is not stored in one place and does not have a center. Instead, the data saved in blockchain is distributed across many different computers, called as nodes.Since no single entity has control over the data, users interact with each other directly without the involvement of a third party.
* **Decentralized Consensus**  
  A blockchain is a decentralized peer-to-peer system which has no central authority to control the exchange of information. Though no involvement of a central administrator keeps the system devoid of corruption, it raises the following questions:
  1. How is a decision made in the blockchain?
  2. How is a transaction added to the chain of blocks?

In a normal centralized model, a central authority or a board of decision-makers take all the required decisions. But it is not possible in the case of blockchain as it has no leader.

The members of a blockchain network need to come to a consensus via “consensus mechanisms” to make decisions. We shall discuss some of the significant consensus algorithms in detail.

* **Smart Contracts**  
  Smart contracts are the building blocks for blockchain-based applications. The concept behind smart contracts is the contractual governance of transactions between two or more participants. It can be verified programmatically with the blockchain, instead of a central authority.Also, smart contracts allow users to control ownership by offering controlled data disclosure.
* **Mining**  
  Mining is defined as the process of adding or validating transactions to the distributed ledger. It mainly involves creating a hash of a block that cannot be forged. As a result, it protects the integrity of the entire system without needing a central system. Miners are the users who utilize the computational power to mine for blocks.

Learning the basics of decentralized technology is not enough, there’s a lot to understand before moving to blockchain development. Let’s discuss some of the concepts which are common yet important for every blockchain enthusiast.

**Following are some of the important concepts that are prerequisite for the blockchain development**

* **Programming Language-** C, C++, Java, JavaScript, Python and Solidity.
* **Data Structures-** Linked List, Hyperledger, Acyclic Graph, HashTable and Associative Array.
* **Security and Encryption-** Secure Hashing Algorithm, Private Key and Public Key Pair.
* **Networking Concepts-** Multi-Threading and Socket Programming.

Whether you are a learner, innovator or entrepreneur, you should also know about the different blockchain consensus algorithms on the basis of which a blockchain platform can be chosen to build a dApp (decentralized application).

**Q. 12 Mentioned below are some of the blockchain consensus algorithms which can be used for blockchain development.**

**Answer: -**

* **Proof of Work**  
  Proof of Work is the first consensus algorithm introduced in the blockchain network. It is used by various blockchain technologies to validate the transactions and add relevant blocks to the chain of a network. As a decentralized ledger contains all information related to the blocks, it is essential to take care of all transactional blocks.

It is the responsibility of miners to manage the transactions blocks which can be done with the process of mining. The concept behind this technique is to solve complicated mathematical problems and provide a solution. Since it requires a lot of computational power to solve a mathematical problem, proof of work has certain limitations. More a network grows, more the power is required.

Firstly, miners have to solve the puzzles to create new blocks and confirm the transactions. The complexity of a puzzle depends on the maximum number of users, overall load and the minimum current power of the network.

Bitcoin is the most common platform where proof of work algorithm is implemented. Ethereum also used the same consensus in 3-4 big projects, but now it has moved on to Proof of Stake.

* **Proof of Stake**  
  Proof of stake is a blockchain consensus algorithm, designed to overcome the drawbacks of the proof of work algorithm.

In Proof of Stake algorithm, each block gets validated before another block is added to the ledger. Miners can participate in the mining process with their coins to stake.

The algorithm has introduced a new type of concept where everyone can mine or validate new blocks based on the coins they hold. So, the more coins an individual has, the more are the chances to become a miner.  
The miners of the network are chosen randomly. If an individual has a specific amount of coins stored in the wallet, then he is qualified to act as a node on the network.

After becoming a node, an individual needs to deposit a specific amount of coins to be qualified as a miner. Voting is done to choose the validators.

Then, the miners can stake the minimum amount needed for the special wallet staking.

New blocks get created which are proportional to the number of coins in the wallet. For instance, if a person owns 10% of all the coins, he can only mine 10% of the new blocks.

* **Proof of Elapsed Time (PoET)**  
  PoET is one of the best consensus algorithms, designed for permissioned blockchain network where you require permission to access the network.

The mining rights or voting principles are decided by the permissions networks.

Since the network requires identification of the miners, the consensus algorithm ensures a secure login into the system.  
Therefore, PoET gives a chance to choose the winners via a fair means only.

The algorithm relies on a special CPU requirement, called “Intel Software Guard Extension”. The Software Guard Extension helps to execute unique codes within the network. Using this system, it ensures that the winning is purely fair.

* **Practical Byzantine Fault Tolerance (PBFT)**  
  PBFT focuses on the state machine. It replicates the system but avoids the main Byzantine general problem.

Now, the question is how PBFT consensus works?

The algorithm assumes from the start that the network could have possible failures and independent nodes might not work properly at certain times.

So, PBFT is designed for asynchronous consensus systems and optimized in an efficient way to deal with the above issues.

Moreover, all the nodes in the system are arranged in a particular order.

Out of all the nodes, one node acts as the primary node while others work as the backup plan. However, all the nodes in the system perform their functions in harmony and interact with one another.

Once you understand the basics of blockchain development, it is the time to understand the various tools that contribute to the blockchain development.

**Q. 13 Explain blockchain development tools which can help ease the development process.**

**Answer: -**

1. **Geth**  
   Geth is a command line interface, used to run a full Ethereum node in Go. The tool is designed to implement an Ethereum node in the Go programming language.By installing and executing Geth, a user can perform the following tasks

* + Mine Ether tokens.
  + Create smart contracts and send transactions on the Ethereum Virtual Machine.
  + Transfer funds between addresses.
  + Track the block history.

Operating systems such as Linux, Mac, and Windows support the installation of Geth. Also, this command line interface supports two types of installations, i.e., Binary and Scripted.

Using Geth, it can be possible to connect to the existing live blockchain and create its blockchain on the basis of provided settings.

1. **Mist**  
   Before the development is started using Ethereum, it is essential to have a place where Ether tokens can be stored and smart contracts can be executed. Mist is a program which is connected to Geth in the background and acts as an interface for the wallet.

Though Mist is widely used for smart contract deployment, you must remember one thing. It is a full node wallet, i.e., one has to download the entire Ethereum blockchain, which is >1Tera Bytes (TB).Mist is supportable on Windows (both 32- and 64-bit), Linux (32- and 64-bit) and Mac. After the node gets fully synced, you will have an option to operate on the testnet or the mainnet.

1. **Remix**  
   Remix is a suite of tools which has been designed to communicate with the Ethereum platform. It is used to debug transactions saved in the Git repository.

A developer needs to connect with an Ethereum node to use tools hosted by Remix.

Remix is comprised of the following tools

* + remix analyzer
  + remix-lib
  + remix-debug
  + remix-tests
  + remixd
  + remix-solidity

Remix IDE is a browser based compiler that allows users to develop Ethereum smart contracts with Solidity language. It also supports testing, deploying and debugging of smart contracts.

1. **Solc (Solidity Compiler)**  
   Solidity is a loosely-typed language which has a syntax similar to that of ECMAScript used for creating the smart contracts on Ethereum blockchain. The role of Solc is to convert the solidity script into a format readable by the Ethereum Virtual Machine.

Solidity Compilers are of two types

* + solc : Coded in C++
  + solc-js : Uses Emscripten to cross-compile from solc C++ to JavaScript

Though both of the above compilers are built from the same source code, they come up with the different results.

1. **Blockchain Testnet**  
   While writing any program for Ethereum Virtual Machine (EVM), it is important to consider the following things:

First, a user has to pay for gas usage and the launch of an application. So, no one would like to pay money for a project that has not been tested.

Secondly, an untested code can have some bugs which can create havoc to the Ethereum blockchain. Also, the information stored on Ethereum blockchain is immutable which cannot be undone.

Therefore, it is good to test a dApp before deploying it on the mainnet. Testnet is quite similar to the Ethereum blockchain which allows developers or users to test the application before deployment.

**Q.14 What are the top blockchain platforms that support blockchain development.**

**Answer: -**

* **Ethereum**Ethereum is an open-source blockchain based distributed computing platform founded by Vitalk Buterin in late 2013. Known for executing smart contracts on the custom-built blockchain, Ethereum uses EVM (Ethereum Virtual Machine) to offer the run-time environment.

No doubt that Ethereum a permissionless (public) blockchain platform, it is built for mass consumption versus restricted access. It has a native cryptocurrency called Ether, which is used to fuel the Ethereum ecosystem. A developer who builds the app on the top of the Ethereum platform has to pay in Ethers to execute transactions and run nodes.

Since Ethereum uses PoW(Proof of Work) consensus algorithm, its speed is comparatively slower as compared to other platforms.

* **Hyperledger Sawtooth**  
  Hyperledger Sawtooth is a modular and enterprise-grade blockchain development platform which can be used to create, execute and deploy distributed ledgers to maintain digital records in a decentralized way.

PoET (Proof of Elapsed Time) consensus algorithm allows Hyperledger Sawtooth platform to integrate with hardware security solutions. Offering a solution to the Byzantine Generals Problem, PoET utilizes the trusted execution environment which enhances the efficiency of existing algorithms like Proof of Work.

Its modular architecture enables applications to select the transaction rules, consensus algorithms, and permissions as per the business needs.

* **Hyperledger Fabric**  
  Intended to build blockchain based applications with a modular architecture, Hyperledger Fabric is another project of Hyperledger designed for permissioned networks. It only enables authorized identities to participate in a blockchain ecosystem.

The architecture of Hyperledger Fabric allows the team of network designers to plug in the preferred components such as consensus and membership services, separating it from other blockchain platforms.

* **EOS**  
  Designed and developed by a private company, Block.one, EOS is a blockchain platform that supports the development of decentralized applications (dApps).

EOS blockchain solution solves the issues of scalability with Ethereum and Bitcoin by offering smart contract capability, decentralized storage of enterprise solutions and hosting services. Transactions to be added to the EOS network accomplish consensus with a delegated proof-of-stake algorithm and multi-threading.

* **Hedera Hashgraph**  
  Based on Directed Acyclic Graph, Hedera Hashgraph is a fast, secure and fair Distributed Ledger Platform that does not require computing a heavy proof of work algorithm.

The transactions to be added to the network are validated via Gossip about Gossip and Virtual Voting consensus algorithm.

**Q.16 what is Digital Identity Verification.**

**Answer:** - Blockchain identity systems enable users to monetize their own data, track how it’s used, and easily share and secure it.

In the off-chain world, “Digital Identity” (D-ID) refers to the aggregated information that is collected by various parties and platforms when a user spends time and conducts activities online. Data such as a user’s search history, social media activity, transaction history, usernames and passwords, call records, SSN, date of birth, credit history, medical history, and other important information routinely finds its way and is stored online, ultimately building a unique profile spread across multiple databases—each user’s Digital Identity.

Users have at their disposal a range of authentication and security tools to protect their data, but even the most secure online platforms can be hacked, leading to exposure of sensitive aspects of a user’s D-ID and putting them and the platforms at risk of identity theft and fraud. In fact, multiple studies have shown that hacked or leaked personal information is among the most [frequently traded](https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/) products on the dark web.

The way D-ID functions on a blockchain, by contrast, is at once more public and more private. [Blockchains](https://chain.link/education-hub/blockchain) are decentralized, immutable ledgers (or databases), allowing for individuals to transact peer-to-peer while maintaining consensus concerning the ledger/data, ultimately creating a source of shared truth. Blockchains are public in the sense that any participant or even outsider can audit every transaction and address, and they’re private in the sense that, unless they’re explicitly permissioned, blockchains require no KYC (Know Your Customer) and users can participate anonymously with their blockchain addresses possessing little or no link to their off-chain identities.

One especially promising use case for blockchain technology is to improve the D-ID experience by applying the best features of blockchain technology to legacy D-ID systems. Though the architectural details vary, a blockchain-based D-ID solution would ideally allow users to selectively choose with whom and when they share their information, keep user information off of databases vulnerable to attack, allow users to better monetize their data, and better preserve user privacy. While this use case might seem trifling at first blush, it offers more than convenience and data security—by some estimates, digital identity and related industries could reach 3% of GDP by [2030](https://blogs.wsj.com/cio/2019/06/21/the-economic-value-of-digital-identity/#:~:text=It%20found%20that%20the%20economic,3%25%20of%20GDP%20by%202030.).

This article will examine the risks and challenges associated with legacy D-ID implementations, break down how blockchain D-ID might solve them, and analyze four specific implementations relying on Chainlink [oracles](https://chain.link/education/blockchain-oracles) to connect personal information with the blockchain.

**Q. 17 Define Current Flaws in D-ID.**

**Answer: -** Though they can often go unnoticed to users who have come to accept them, the flaws of legacy D-ID systems are both systemic and pernicious. D-ID is a crucial element to making many of the online systems people rely on for everyday life work, but at nearly every step—from the collection, storage, and sale of data—D-ID is rife with security, privacy, and even ethical concerns. Ultimately, these problems can roughly be grouped into three categories: data monetization, data access, and data storage.

Data Monetization

An important part of D-ID is the data surreptitiously gathered by major internet platforms on a user’s behavior, habits, and biographical information. A search engine, for instance, might gather data about a user’s interests to tailor ads for them, or a social media site might sell information natively created by users to interested parties such as political campaigns. Because the details of these activities are often buried in terms-of-use agreements, users of these platforms ubiquitously and unwittingly enrich platforms with time spent ostensibly in leisure.

This process where users, by engaging in normal habits, unknowingly provide platforms with information that is then subsequently monetized is frequently referred to “free labor.” Proponents of free labor argue that this data monetization is a natural trade-off for access to what are often free services/platforms, and that they eventually benefit the user by allowing the platforms to grow faster and provide better user experiences.

However, free labor presents a host of ethical and privacy issues, often revolving around users being unclear about what data is being gathered, to whom it’s being sold, or where it’s being stored. Though some countries have attempted to place regulations on the data that can be collected by major platforms, free labor remains a rampant issue, with users all across the Internet unsure of what data is being gathered and what’s being done with it.

Data Access

Certain Internet platforms and services require a more complete D-ID profile to access than others. Social media sites may require just an email address (though they’ll subsequently build a profile on a user), while a lending service or a government agency might want a full financial or personal history before providing access and services through their portal. As a result, users are often forced to provide the same information about themselves over and over across different platforms. While the separation of databases may prevent a more catastrophic breach by isolating an attack, each database storing important user information ultimately increases the attack surface of a user’s data.

This puts users in a difficult position, having to choose between time-consuming processes and bureaucracy or storing their information for repeated use on databases that might potentially be vulnerable to attack. Additionally, this system also creates headaches for the platforms as well: government agencies might store redundant information across multiple servers, which leads to cost inefficiency, and other platforms might become more vulnerable to scams or theft as a result of user data leaks. In many instances, the platforms are ultimately the responsible parties for any financial losses associated with identity theft.

Data Security

As mentioned above, users frequently propagate information about themselves online, including financial information in order to make purchases or gain access to services. Access and security rarely go hand-in-hand, and the same holds true for D-ID—each website that stores information about a user presents a new attack vector through which their information might be stolen.

Given the level of the threat, one would expect that platforms would invest in superior security and privacy infrastructure. However, in spite of security efforts statistics indicate that data protection problems are getting worse, not better: upwards of[10% of the population](https://www.consumeraffairs.com/finance/identity-theft-statistics.html)is affected by identity theft every year, and that number is on the rise during the pandemic.

**Q. 18 Explain Blockchain-Based D-ID Solutions.**

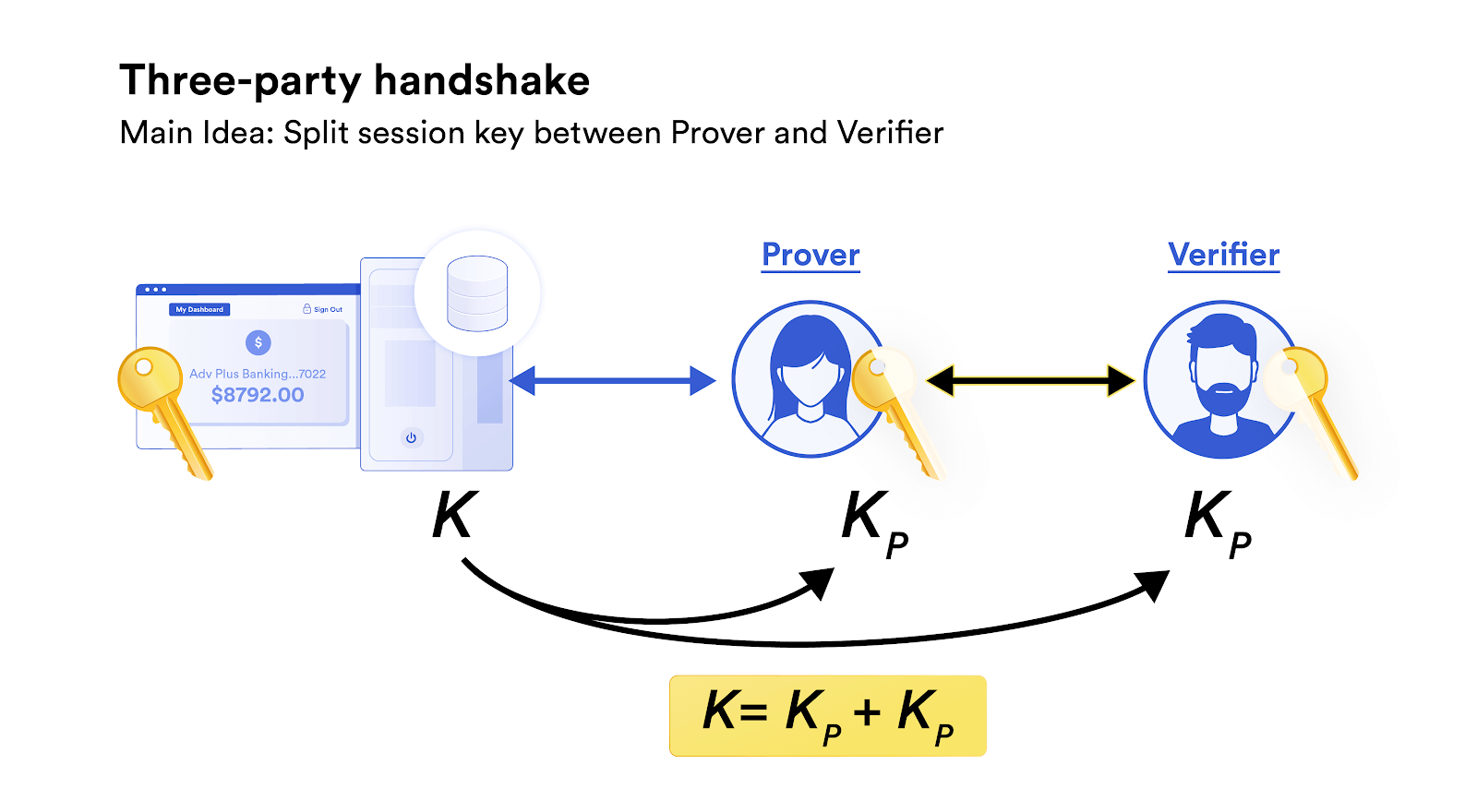
**Answer: -** Because of these flaws, D-ID is a space ripe for disruption from blockchain technology. By using blockchains to architect superior D-ID systems, many of the most glaring problems with D-ID can be solved and whole new use cases can be enabled.

The key features of a blockchain-based D-ID system would include: the ability for users to monetize the information they natively create and track how their information is being used; the ability to readily and easily share D-ID information; and the ability to keep that data secure. There are a range of unique approaches towards achieving these goals—including the potential of doing away with off-chain identities entirely—and each leverage blockchain in different ways.

DECO

One blockchain-based D-ID system is Chainlink’s privacy preserving oracle technology [DECO](https://arxiv.org/pdf/1909.00938.pdf)—developed by Chainlink Labs Chief Scientist Ari Juels, researcher Fan Zhang, and others. While new D-ID storage solutions may alter how data is stored, the reality is that a lot of data is still stored in trusted databases. Many users/institutions may prefer the security of entrusting a high-security custodian to protect that data, especially governments and large enterprises.

DECO allows oracles to attest to the validity of information in trusted databases/systems without exposing it to the public or even the oracle itself using a cryptographic technique known as Zero Knowledge Proofs. Essentially, the oracle can join a user-initiated web session to attest to some requested information— possibly to verify someone’s identity, approve their financial information, or check key government records. Importantly, that data never leaves the secure, user-selected database, allowing a user to store their D-ID information in certain locations they trust and set up selective access, as opposed to propagating it to a variety of systems with weak guarantees on access control. This allows for a privacy-preserving plug-and-play option that combines the usability of legacy systems with the security of blockchain.



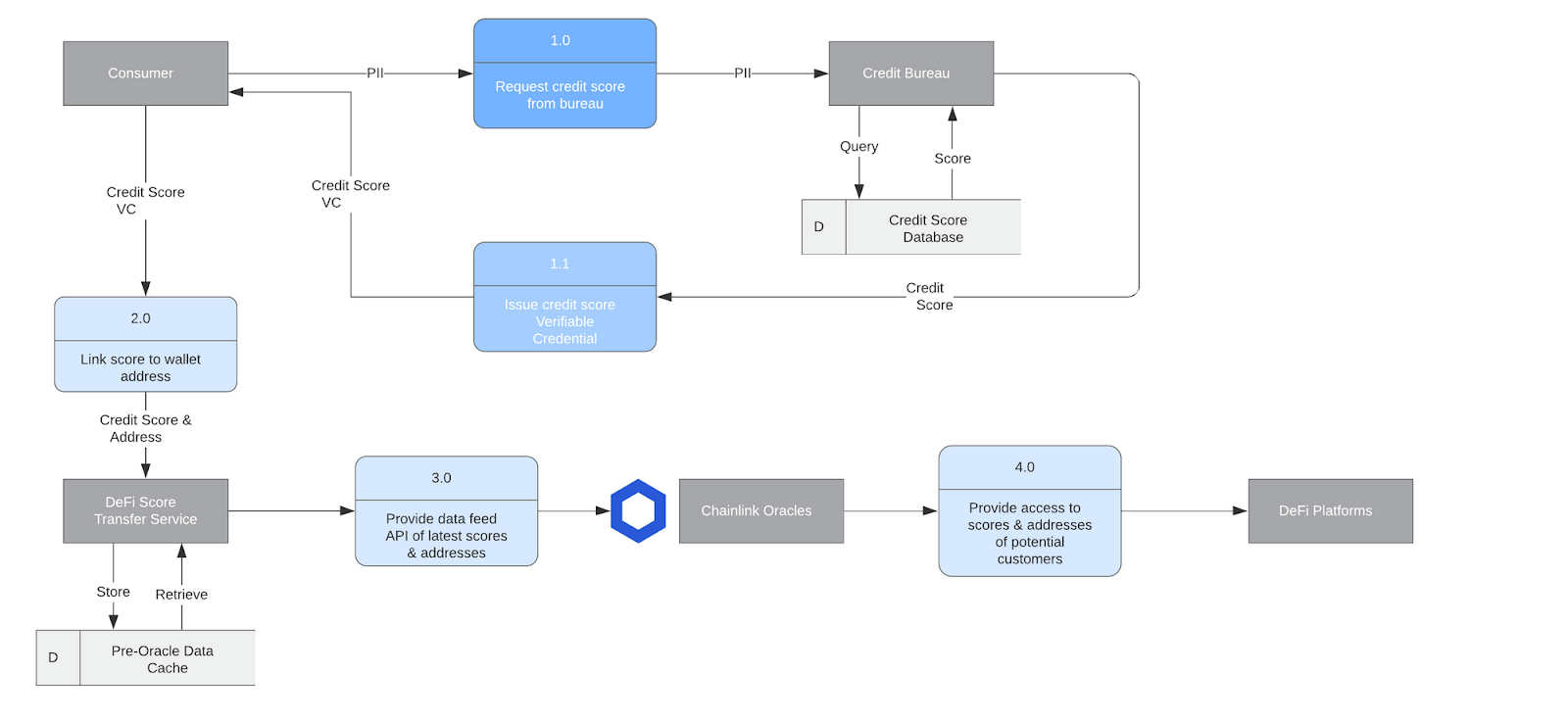
One of DECO’s main techniques involves a three-party handshake – a method in which the Prover (user) and Verifier (oracle) can combine their public TLS keys and form a combined request for data, without the Verifier ever receiving said data.

DECO’s privacy-preserving technology also allows for use cases that would otherwise have been impossible, such as big data medical studies. For years researchers have been excited about the potential of applying machine learning and computational analysis to large medical datasets, hoping to use these tools to make discoveries and breakthroughs that human analysis wouldn’t be able to find. However, the privacy and security concerns of patient data have long been a roadblock. DECO would allow researchers selective access to the data they need while complying with HIPA regulations and without putting that data at risk, potentially enabling a new era of medical research.

Bloom

Another example of a project using blockchain technology to enhance D-ID is Bloom, a decentralized identity protocol that allows users to claim, control, and selectively share their financial data while retaining full ownership via a decentralized architecture.

Bloom works by taking user-provided data and verifying each user’s identity, and then subsequently writing that data to the blockchain as an encrypted hash. This allows user information to be stored on a public ledger/source of truth while simultaneously maintaining privacy of it. It’s especially useful for financial information, which is one of Bloom’s core areas of focus—a recent [blog post](https://bloom.co/blog/bloom-integrates-with-chainlink-decentralized-finance/) from Bloom laid out how Chainlink oracles help connect credit scores to [DeFi](https://chain.link/education/defi) protocols.



**Q. 19 How Chainlink decentralized oracles connect credit scores to DeFi protocols.**

**Answer :-** “Bloom started as a protocol using [smart contracts](https://chain.link/education/smart-contracts) and Ethereum addresses to uniquely identify individuals and enable them to claim, store, and share verified identity attributes, with the goal of decentralizing the credit bureau model,” says Isaac Patka, CTO of Bloom. “As the technology evolved we joined forces with the larger decentralized/self-sovereign identity community to develop open and interoperable standards for identifying users, issuing credentials, and exchanging information. The identity standards have now matured to the point that we can take this technology to market and drive global impact. We are excited to realize our original vision of extending financial inclusion, and using platforms like Chainlink to bridge the gap between the traditional and decentralized worlds.”

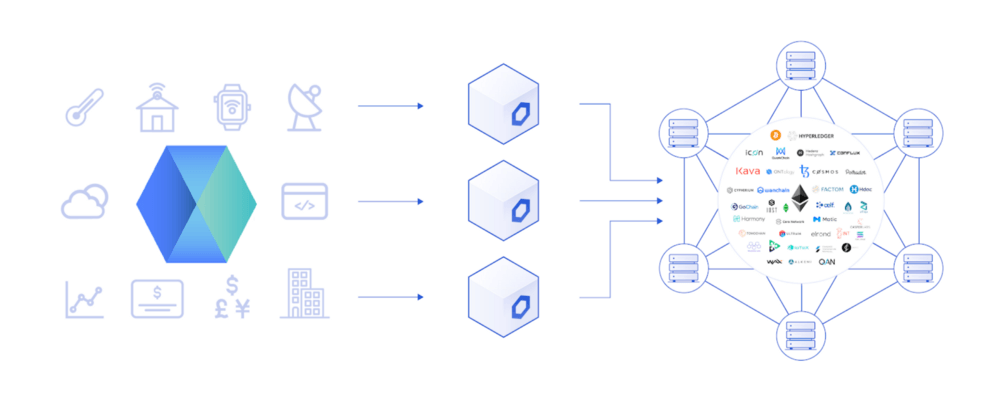
Unstoppable Domains

Unstoppable Domains is decentralized blockchain-based protocol for registering and hosting Internet [domain names as non-fungible ERC721 tokens](https://blog.chain.link/how-to-create-nft-domain-names/) on the Ethereum blockchain. Unstoppable Domains [recently announced](https://hackernoon.com/making-crypto-payments-less-scary-pjv3z2f) a new feature that uses Chainlink oracles to link Twitter users to specific domains, making it easy to identify and confirm a user’s public address based on their social media account. Additionally, users can send payments directly to the domains, bypassing often confusing Ethereum addresses for a superior UI/UX experience.

What makes this solution unique is that it can potentially bypass real-world information entirely. Twitter users can remain anonymous, but still have a named Internet domain linked to them that can send and receive blockchain-based payments. This allows for secure, highly intuitive transfer of value between parties whose identities are potentially entirely digital and don’t have to be stored in any centralized database.

Decentr

Decentr is a project that aims to provide a Web3 version of credit scores—what they call a “Personal Data Value” (PDV). Each user’s PDV would be sourced from a potential combination of social media activity, on-chain activity such as their total owned assets and history of repaying loans, and real-world data such as KYC/AML information. As discussed Decentr’s [blog post](https://medium.com/@DecentrNet/decentr-integrates-chainlink-to-provide-user-centric-social-reputation-scores-to-defi-311d12ed4b68), Chainlink oracles can supply this data to DeFi protocols across any blockchain, and users with high PDV values could potentially receive less collateralized or even collateral-free loans.



Decentr integrates with Chainlink to provide user-centric social reputation scores to DeFi.

Like Unstoppable Domains, this approach not only finds a way to securely connect off-chain data to D-ID using blockchain, but also bolsters the blockchain identity experience by taking valuable on-chain data and using it to create a D-ID profile of users. Privacy-focused users could potentially bypass using real-world information all together, and instead build their PDV value solely from their on-chain metrics.

**Q. 20 Define BLOCKCHAIN NEUTRALITY.**

**Answer: -** Blockchain technology is transforming how markets work. Blockchains eliminate the need for trusted gatekeepers like banks to execute, verify, and record transactions. In the  
financial markets, their disruptive potential threatens both Wall Street banks and Silicon Valley venture capitalists. How blockchain technology is regulated will determine whether it  
encourages or inhibits competition. Some blockchain applications present serious fraud and systemic risks, complicating regulation. This Article explores the antitrust and competition policy challenges blockchain presents and proposes regulatory strategy, modelled on Internet regulation and net neutrality principles, to unlock blockchain’s competitive potential. It contends that financial regulators should promote blockchain competition—and the resulting market decentralization—except in cases where specific applications are shown to harm consumers or threaten systemic safety. Regulators also should ensure open access and non-  
discrimination on dominant blockchain networks. This approach will not only serve traditional antitrust goals of lowering prices and promoting innovation, but it also might  
achieve broader economic and social reform by reducing the power and influence of the biggest financial institutions.

DIGITAL ART:

Crypto art is a blanket term coined to represent the fusion of art and [blockchain technology](https://cointelegraph.com/blockchain-for-beginners/how-does-blockchain-work-everything-there-is-to-know). As a sub ecosystem within the world of cryptocurrencies, crypto art intends to preserve immutable versions of digital art such as music albums, paintings, awards and a wide range of memorabilia.

Crypto art is preserved on the blockchain in [the form of nonfungible tokens](https://cointelegraph.com/nonfungible-tokens-for-beginners), or NFTs, and are usually tied up with a monetary value. Just like traditional art forms, the value of crypto art or NFTs is heavily influenced by the credibility of the creator, the rarity of the art and its demand in the collector’s market.

As a collectible, NFTs and similar forms of digital art are capable of being publicly verified for authenticity and change of ownership. This allows every piece of art to be verifiably unique and hold a corresponding monetary value. Let’s dive deeper into the world of crypto art.

**Q. 21 Who are the crypto artists?**

**Answer: -** The biggest drivers of the crypto art landscape are the artists that create/recreate pieces to be stored over the blockchain. Although NFTs can represent numerous aspects of the digital world, the first step begins with the creation of digital artwork. Digital art can be created by using readily-available software and a personal computer in the form of GIF, JPEG, videos, 3D images and similar art forms.

While the aforementioned digital art can be easily replicated and distributed over the internet, crypto artists need to certify and mint a nonfungible token that is linked to the authenticity of the art created. Once certified, the art can then be uploaded to various marketplaces and marketed to potential buyers.

It is important to note that crypto art is also subject to copyright laws and artists are expected to create, mint and sell unique NFTs while respecting the ownership of other artworks.



## Metaverse

The term metaverse was coined in 1992 by Neal Stephenson, the author of the science fiction novel Snow Crash. This was the first time someone envisioned a full-interactable virtual world consisting of human avatars and 3D digital objects.

[Metaverse is the most popular implementation](https://cointelegraph.com/blockchain-for-beginners/what-is-metaverse-in-blockchain-a-beginners-guide-on-an-internet-enabled-virtual-world) of crypto art or NFTs, which makes use of digital art to represent objects in a fully-functional virtual world. The Metaverse allows users to create, own, create, purchase and sell virtual versions of shoes, clothes, property and other belongings.

A metaverse can also represent social communities where people from all over the world can participate in online meetups for conferences, meetings and parties. In a typical metaverse setting, users can interact with each other and co-participate in virtual reality (VR) events such as dancing to music or attending yoga classes in groups.

Metaverses has also found use cases in the gaming industry as developers create open-world games around the rising digital ecosystem. By infusing gamification, metaverses can be modified to depict interactive virtual worlds explorable through user-created avatars.

Given the untapped potential of possibilities within metaverses, major social media and tech corporations continue to explore various use cases primarily aimed at improving customer engagement. For example, social media giant Facebook renamed itself “Meta” to be more aligned with the development of a metaverse. Following suit, numerous tech giants are also exploring metaverse capabilities to identify the various revenue streams and customer engagement services.

## Nonfungible tokens (NFT)

Nonfungible tokens are what make crypto art possible. While comparable to any other form of digital images including JPEG, GIF and 3D images, NFTs contain metadata that can help prove its value and ownership over a public blockchain.

Given the endless possibilities offered by digitalization, NFTs have evolved into representing real-world objects in metaverses and other virtual worlds. Online virtual stores facilitate retail purchases of digital clothes, shoes, property and other assets and merchandise.

Moreover, the true market value of NFTs is dictated by the rarity and the public demand for a particular collection or entity. Some of the mainstream examples of NFT adoption include the launch of music albums and the issuance of awards and fan tokens in various sport events.

In addition to representing aspects of the real world, artists make the most of this budding landscape to create art and market it to potential buyers across the globe. This also brings the opportunity for enthusiasts to recreate popular paintings and offer collectors a piece of priceless history.

**Q. 22 How much does it cost to hang the crypto art on your wall?**

**Answer: -** While crypto art can be replicated and copied by simply downloading the image or taking a screenshot, the process leaves out the most important feature of the art, i.e., the metadata or the proof of its uniqueness.

Every digital art needs to be assigned a unique ID before it can be called NFT and possess a monetary value. As a result, the unique ID of the NFTs is what makes the arts one-of-a-kind, confirming the legitimacy of the art’s value and ownership. The typical prices of minting an NFT can range from as low as $1.00 to an average of $900, depending on the service provider and the blockchain host. However, unrealistic gas prices can drive up the NFT minting costs even higher.

The unique ID of an NFT artwork can be cross-checked across a network of public blockchains. When crypto art gets sold or transferred to a different user, the metadata gets timestamped over the blockchain network. Depending on the rarity and collector’s demand of the piece, an NFT can range anywhere from a few dollars to millions.

NFT marketplaces help the creator mint digital art into a nonfunglible token. The process typically involves the use of a native blockchain cryptocurrency wallet and cryptocurrency payment. Minting requires the creator to pay transaction fees or gas fees for updating the blockchain with the metadata about the crypto art in question, determined by the blockchain network and the stress or the current transactional capacity of the blockchain.

## Weighing in the risks and rewards

The NFT marketplace, while rewarding, has opened new potential avenues for scammers and bad actors that target unsuspecting investors and collectors. Just like any other ecosystem that involves cryptocurrency and blockchain technology, investors and enthusiasts are advised to research heavily on the NFTs before making any commitments or purchases.

It is equally important for investors to confirm the metadata of the NFTs on their corresponding blockchains. Metadata is a term used to describe additional information about a particular object or an instance which, in the case of NFTs, involves information about minting, blockchain host, ownership and the creator details. The information available on the blockchain can be regarded as the only way to confirm the legitimacy of a crypto art offering.

As discussed, the credibility and the value of NFTs are directly linked to their creators and the demand in the resale market. That being said, even though the NFTs may check out in terms of authenticity, it does not guarantee high (or any) resale value. The resale value of NFTs is purely determined by the investor sentiment attached to the art.

**Q. 23 Can crypto art be copied?**

**Answer: -** Contrasting to the popular belief that replicating crypto art is as simple as saving a copy of the image or video locally on a computing device, copying crypto art is technically impossible. For example, when a user attempts to “save” a crypto art, the person ends up saving an identical copy of the image but misses out on capturing the information that makes the NFT component of any digital art.

In many cases, the artist may choose to retain the copyright ownership of an NFT, which allows the artist to create and sell multiple copies of the same art. However, the metadata helps differentiate the ownership of similar-looking NFTs and ensures the credibility of the creator.

As discussed earlier, crypto art (just like any other form of art) is subject to copyright and wrongly claiming to be the creator can have negative consequences depending on the law of the land.

## A peek into the future of NFTs, metaverse and crypto art

The future of crypto art will be determined by the people that believe in the ecosystem and its extent of mainstream adoption. Given the involvement of popular artists, musicians, sports persons and celebrities, crypto art has fortunately attracted a large number of people willing to buy, sell and collect art in the form of NFTs.

The existing use cases of the crypto art ecosystem involve art and interactive virtual worlds. With increased adoption, NFTs are slowly bleeding into the world of virtual asset purchases such as purchasing online versions of limited-edition clothes, property and so on.

While the world of cryptocurrencies, especially crypto art, is yet to be tested for its full potential, the budding technology has already altered the way we look at precious collectibles and art in a virtual setup. As for its future, crypto art is well-positioned to be treated as an instrument of a virtual representation of every aspect of our day-to-day lives.

**BLOCKCHAIN ENVIRONMENT:**

Blockchain, a digital ledger technology, is widely known for its application to cryptocurrencies. Introduced in 2008 to serve as a public transaction ledger for Bitcoin, the technology has given rise to hundreds of cryptocurrencies (e.g. Ethereum, Ripple, NEO, Litecoin), as well as having other emerging applications in diverse fields, including supply chains, digital content, patents, smart contracts, governance and e-voting (EPRS, 2017).

Understanding the basics of blockchain technology is essential to assess its implications, which are potentially huge and transformative for society, the economy and the environment. The European Union Agency for Network and Information Security (ENISA) defines blockchain as:

… a public ledger consisting of all transactions taking place across a peer-to-peer network. It is a data structure consisting of linked blocks of data … This decentralised technology enables the participants of a peer-to-peer network to make transactions without the need of a trusted central authority and at the same time relying on cryptography to ensure the integrity of transactions.

(ENISA, 2019)

In contrast to the traditional ledgers used by banks and governments for centuries, which are centralised and inaccessible, blockchain ledgers are decentralised and transparent (EPRS, 2017). There is no central authority acting as the exclusive manager of the ledger, with sole responsibility for storage, updates and verification of transactions. On the contrary, all participants of the blockchain network hold a copy of the ledger, and transactions — although encrypted — are visible to all.

Although participants may not know each other, such a decentralised ledger system is viable because it is made trustworthy and secure by design. Blockchain stores, shares and synchronises data as ‘chains of blocks’ using cryptographic techniques. Blocks represent recorded transactions, and each new block of transactions is linked to the previous ones, thus creating an ever growing chain (Nakamoto, 2008). The creation of each new block must be approved by all network participants. This is achieved thanks to a predefined ‘consensus mechanism’ that sets the rules for the verification, validation and addition of transactions to the ledger (JRC, 2018). The most common approach is ‘mining’, which relies on the ‘proof-of-work’ mechanism. To add a block of transactions to a blockchain, participants compete to find a solution to a difficult mathematical problem based on a cryptographic algorithm (EPRS,2017). When a ‘miner’ finds the solution, and after verification from other participants, the block is added to the blockchain. All copies of the ledger are updated, making the new changes permanent.

Furthermore, each block has a timestamp as well as a unique hash value referring to previous blocks. The authenticity and integrity of transactions themselves are ensured by standard public-private key cryptography. With constant updates and validation made to the blockchain, as well as inspection of the complete history of transactions open (at least potentially) to everyone, unauthorised changes or tampering are almost impossible (JRC, 2018). All these features make the ledger unique and immutable, ensuring trust among participants to operate their transactions. In addition, these transactions can be executed automatically, without the need for human intervention, thanks to self-executing computer codes — named ‘smart contracts’ — that contain the terms of contracts and are stored in the blockchain.

‘Permissionless’ blockchains, of the sort just described, allow anyone to access, verify and add transitions. But it is also possible to set up a ‘permissioned’ blockchain where access to and the validation or addition of transactions are restricted to a more limited group of people (Kouhizadeh and Sarkis, 2018).