Blockchain could be a data structure that could be a growing list of information blocks. The knowledge blocks area unit coupled along, such recent blocks can't be removed or altered. Blockchain is the backbone Technology of the Digital Cryptocurrency Bitcoin.

What is Blockchain?

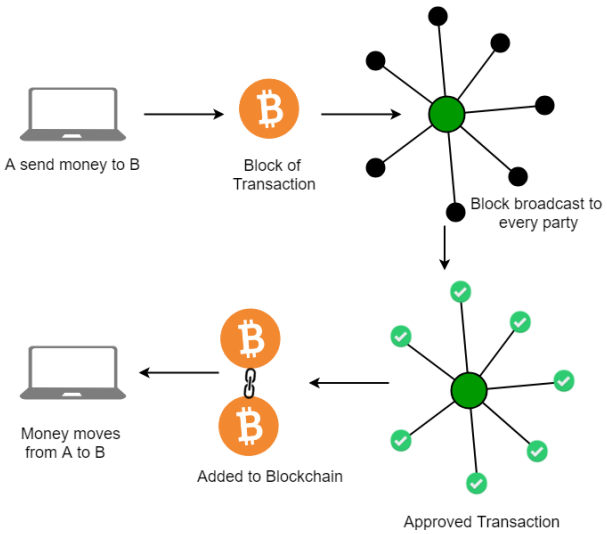
The blockchain is a distributed database of records of all transactions or digital events that have been executed and shared among participating parties. Each transaction is verified by the majority of participants of the system.

It contains every single record of each transaction. Bitcoin is the most popular cryptocurrency an example of the blockchain. Blockchain Technology first came to light when a person or group of individuals name 'Satoshi Nakamoto' published a white paper on "*Bitcoin: A peer-to-peer electronic cash system*" in 2008.

Blockchain Technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible. Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction.

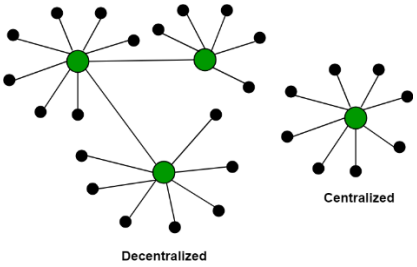
How does Blockchain Technology Work?

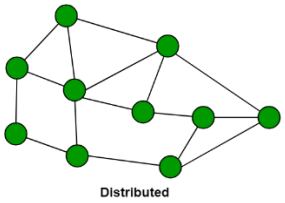
One of the famous use of Blockchain is Bitcoin. Bitcoin is a cryptocurrency and is used to exchange digital assets online. Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the Internet. Each transaction protects through a digital signature.



Blockchain Decentralization

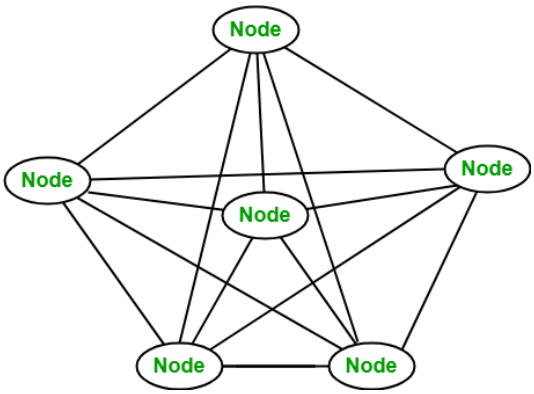
There is no Central Server or System which keeps the data of the Blockchain. The data is distributed over Millions of Computers around the world which are connected to the Blockchain. This system allows the Notarization of Data as it is present on every Node and is publicly verifiable.





Blockchain nodes

A node is a computer connected to the Blockchain Network. Node gets connected with Blockchain using the client. The client helps in validating and propagating transactions onto the Blockchain. When a computer connects to the Blockchain, a copy of the Blockchain data gets downloaded into the system and the node comes in sync with the latest block of data on Blockchain. The Node connected to the Blockchain which helps in the execution of a Transaction in return for an incentive is called Miners.



Disadvantages of the current transaction system:

- Cash can only be used in low-amount transactions locally.
- The huge waiting time in the processing of transactions.
- The need for a third party for verification and execution of Transactions makes the process complex.
- If the Central Server like Banks is compromised, the whole system is affected including the participants.
- Organizations doing validation charge high process thus making the process expensive.

Building trust with Blockchain: Blockchain enhances trust across a business network. It's not that you can't trust those who you conduct business with it's that you don't need to when operating on a Blockchain network. Blockchain builds trust through the following five attributes:

- **Distributed:** The distributed ledger is shared and updated with every incoming transaction among the nodes connected to the Blockchain. All this is done in real time as there is no central server controlling the data.
- **Secure:** There is no unauthorized access to Blockchain made possible through Permissions and Cryptography.
- **Transparent:** Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data. They themselves can verify the identities without the need for mediators.
- **Consensus-based:** All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.
- **Flexible:** Smart Contracts which are executed based on certain conditions can be written into the platform. Blockchain Networks can evolve in pace with business processes.

What are the benefits of Blockchain?

- **Time-saving:** No central Authority verification is needed for settlements making the process faster and cheaper.
- **Cost-saving:** A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced. Transaction efforts are minimized as every participant has a copy of the shared ledger.
- **Tighter security:** No one can tamper with Blockchain Data as it is shared among millions of Participants. The system is safe against cybercrimes and Fraud.
- **Collaboration:** It permits every party to interact directly with one another while not requiring third-party negotiation.
- **Reliability:** Blockchain certifies and verifies the identities of every interested party. This removes double records, reducing rates and accelerating transactions.

Application of Blockchain

- Leading Investment Banking Companies like Credit Suisse, JP Morgan Chase, Goldman Sachs, and Citigroup have invested in Blockchain and are experimenting to improve the banking experience and secure it.
- Following the Banking Sector, the Accountants are following the same path. Accountancy involves extensive data, including financial statements spreadsheets containing lots of personal and institutional data. Therefore, accounting can be layered with blockchain to easily track confidential and sensitive data and reduce human error and fraud. Industry Experts from Deloitte, PwC, KPMG, and EY are proficiently working and using blockchain-based software.

- Booking a Flight requires sensitive data ranging from the passenger's name, credit card numbers, immigration details, identification, destinations, and sometimes even accommodation and travel information. So sensitive data can be secured using blockchain technology. Russian Airlines are working towards the same.
- Various industries, including hotel services, pay a significant amount ranging from 18-22% of their revenue to third-party agencies. Using blockchain, the involvement of the middleman is cut short and allows interaction directly with the consumer ensuring benefits to both parties. Winding Tree works extensively with Lufthansa, Air France, Air Canada, and Etihad Airways to cut short third-party operators charging high fees.
- Barclays uses Blockchain to streamline the Know Your Customer (KYC) and Fund Transfer processes while filling patents against these features.
- Visa uses Blockchain to deal with business-to-business payment services.
- Unilever uses Blockchain to track all their transactions in the supply chain and maintain the product's quality at every stage of the process.
- Walmart has been using Blockchain Technology for quite some time to keep track of their food items coming right from farmers to the customer. They let the customer check the product's history right from its origin.
- DHL and Accenture work together to track the origin of medicine until it reaches the consumer.
- Pfizer, an industry leader, has developed a blockchain system to keep track of and manage the inventory of medicines.
- The government of Dubai looking forward to making Dubai the first-ever city to rely on entirely and work using blockchain, even in their government office.
- Along with the above organizations, leading tech companies like Google, Microsoft, Amazon, IBM, Facebook, TCS, Oracle, Samsung, NVIDIA, Accenture, and PayPal, are working on Blockchain extensively.

Is Blockchain Secure?

Nowadays, as the blockchain industry is increasing day by day, a question arises is Blockchain safe? or how safe is blockchain? As we know after a block has been added to the end of the blockchain, previous blocks cannot be changed. If a change in data is tried to be made then it keeps on changing the Hash blocks, but with this change, there will be a rejection as there are no similarities with the previous block.

Just imagine there is a who hacker runs a node on a blockchain network, he wants to alter a blockchain and steal cryptocurrency from everyone else. With a change in the copy, they would have to convince the other nodes that their copy was valid.

They would need to control a majority of the network to do this and insert it at just the right moment. This is known as a 51% attack because you need to control more than 50% of the network to attempt it.

Timing would be everything in this type of attack—by the time the hacker takes any action, the network is likely to have moved past the blocks they were trying to alter.

Blockchain project ideas

Here are a few project ideas for beginners looking to learn more about blockchain technology:

1. **Cryptocurrency Wallet:** Create a simple cryptocurrency wallet application that allows users to send and receive digital assets.
2. **Blockchain Explorer:** Develop a web-based application that allows users to view and search the transactions on a specific blockchain.
3. **Smart Contract:** Implement a simple smart contract on the Ethereum blockchain that can be used to manage a digital token or asset.
4. **Voting System**: Create a blockchain-based voting system that allows for secure and transparent voting while maintaining voter anonymity.
5. **Supply Chain Management:** Develop a blockchain-based system for tracking the movement of goods and services through a supply chain, providing greater transparency and traceability.
6. **Decentralized marketplace:** Create a decentralized marketplace using blockchain technology where the goods and services can be directly bought by the customers without any intermediary.
7. **Identity Management:** Create a decentralized digital identity management system that allows users to control their personal information and share it securely with others.

These are just a few examples, there are many other possibilities to explore within Blockchain technology.

Future Scope of Blockchain Technology

Finance, supply chain management, and the Internet of Things are just a few of the sectors that blockchain technology has the power to upend (IoT). The following are some potential uses for blockchain in the future:

- Digital Identity: Blockchain-based digital IDs might be used to store personal data safely and securely as well as offer a means of establishing identity without the need for a central authority.
- Smart Contracts: A variety of legal and financial transactions could be automated using smart contracts, self-executing contracts with the terms of the agreement put straight into lines of code.

- Decentralized Finance (DeFi): Using blockchain technology, decentralized financial systems might be built that support peer-to-peer transactions and do away with conventional intermediaries like banks.
- Supply Chain Management: Blockchain technology can be applied to a permanent record of how goods and services have been moved, enabling improved openness and traceability across the whole supply chain.
  -Internet of Things (IoT): Blockchain technology may be used to build decentralized, secure networks for IoT devices, enabling them to exchange data and communicate with one another in an anonymous, safe manner.

In general, blockchain technology is still in its early stages and has a wide range of potential applications.

Advantages of Blockchain Technology:

1. Decentralization: The decentralized nature of blockchain technology eliminates the need for intermediaries, reducing costs and increasing transparency.
2. Security: Transactions on a blockchain are secured through cryptography, making them virtually immune to hacking and fraud.
3. Transparency: Blockchain technology allows all parties in a transaction to have access to the same information, increasing transparency and reducing the potential for disputes.
4. Efficiency: Transactions on a blockchain can be processed quickly and efficiently, reducing the time and cost associated with traditional transactions.
5. Trust: The transparent and secure nature of blockchain technology can help to build trust between parties in a transaction.

Disadvantages of Blockchain Technology:

1. Scalability: The decentralized nature of blockchain technology can make it difficult to scale for large-scale applications.
2. Energy Consumption: The process of mining blockchain transactions requires significant amounts of computing power, which can lead to high energy consumption and environmental concerns.
3. Adoption: While the potential applications of blockchain technology are vast, adoption has been slow due to the technical complexity and lack of understanding of the technology.
4. Regulation: The regulatory framework around blockchain technology is still in its early stages, which can create uncertainty for businesses and investors.
5. Lack of Standards: The lack of standardized protocols and technologies can make it difficult for businesses to integrate blockchain technology into their existing systems.

6. Overall, the advantages of blockchain technology are significant and have the potential to revolutionize many industries. However, there are also several challenges and disadvantages that must be addressed before the technology can reach its full potential.

Blockchain and Distributed Ledger Technology (DLT)

A blockchain is a digital ledger of transactions that are distributed across the entire network of computers (or nodes) on the blockchain. Distributed ledgers use independent nodes to record, share, and synchronize transactions in their respective electronic ledgers instead of keeping them in one centralized server. A blockchain uses several technologies like digital signatures, distributed networks, and encryption/ decryption methods including distributed ledger technology to enable blockchain applications.

Blockchain is one of the types of DLT in which transactions are recorded with an unchangeable cryptographic signature called a hash. That is why distributed ledgers are often called blockchains.

What is Distributed Ledger Technology (DLT)?

Distributed Ledger Technology (DLT) is centred around an encoded and distributed database where records regarding transactions are stored. A distributed ledger is a database that is spread across various computers, nodes, institutions, or countries accessible by multiple people around the globe.

Features:

1. **Decentralized:** It is a decentralized technology and every node will maintain the ledger, and if any data changes happen, the ledger will get updated. The process of updating takes place independently at each node. Even small updates or changes made to the ledger are reflected and the history of that change is sent to all participants in a matter of seconds.
2. **Immutable:** Distributed ledger uses cryptography to create a secure database in which data once stored cannot be altered or changed.
3. **Append only:** Distributed ledgers are append-only in comparison to the traditional database where data can be altered.
4. **Distributed:** In this technology, there is no central server or authority managing the database, which makes the technology transparent. To counter the weaknesses of having one ledger to rule all, So that there is no one authoritative copy and have specific rules around changing them. This would make the system much more transparent and will make it a more decentralized authority. In this process, every node or contributor of the ledger will try to verify the transactions with the various consensus algorithms or voting. the voting or participation of all the nodes depends on the rules of that ledger. In the case of bitcoin, the Proof of Work consensus mechanism is used for the participation of each node.
5. **Shared:** The distributed ledger is not associated with any single entity. It is shared among the nodes on the network where some nodes have a full copy of the ledger while some nodes have only the necessary information that is required to make them functional and efficient.

6. **Smart Contracts:** Distributed ledgers can be programmed to execute smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This allows for transactions to be automated, secure, and transparent.
7. **Fault Tolerance:** Distributed ledgers are highly fault-tolerant because of their decentralized nature. If one node or participant fails, the data remains available on other nodes.
8. **Transparency:** Distributed ledgers are transparent because every participant can see the transactions that occur on the ledger. This transparency helps in creating trust among the participants.
9. **Efficiency:** The distributed nature of ledgers makes them highly efficient. Transactions can be processed and settled in a matter of seconds, making them much faster than traditional methods.
10. **Security:** Distributed ledgers are highly secure because of their cryptographic nature. Every transaction is recorded with a cryptographic signature that ensures that it cannot be altered. This makes the technology highly secure and resistant to fraud.

How DLT Can Replace Traditional Book-Keeping Methods?

Distributed ledger technology has the potential to effectively improve these traditional methods of bookkeeping by updating and modifying fundamental methods of how data is collected, shared, and managed in the ledger. To understand this, traditionally paper-based and conventional electronic ledgers were used to manage data that had a centralized point of control. These types of system require high computing resource and labour to maintain ledgers and also had many points of failure. Points of failure like:

1. Mistakes made during data entry.
2. Manipulation of data could happen which increases the risk of errors.
3. Other participants contributing data to the central ledger will not able to verify the legitimacy of data coming from other sources.

However, DLT allows real-time sharing of data with transparency which gives trust that data in the ledger is up to date and legitimate. Also Distributed Ledger Technology eliminates the single point of failure which prevents data in the ledger from being manipulations and errors. In DLT, there is no need for a central authority to validate transactions here different consensus mechanisms are used to validate transactions which eventually makes this process very fast and real-time. Similarly, DLT can reduce the cost of transactions because of this process.

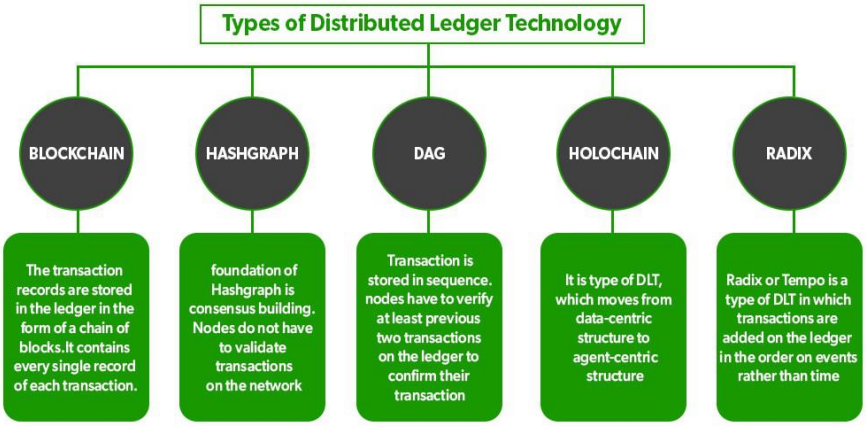
Types of Distributed Ledger Technology

The Distributed Ledgers can be categorized into three categories:

1. **Permissioned DLT:** Nodes have to take permission from a central authority to access or make any changes in the network. Mostly these types of permissions include identity verification.
2. **Permissionless DLT:** There is no central authority to validate transactions, rather existing nodes are collectively responsible for validating the transactions. Various consensus mechanisms are used to validate transactions based on predefined algorithms. In the case of bitcoin proof of work consensus mechanism is used.
3. **Hybrid DLT:** It is combined with both permissionless and permissioned DLTs and can benefit from both of them.

Below are some of the types of DLT:

1. **Blockchain:** In this type of DLT, transactions are stored in the form chain of blocks and each block produces a unique hash that can be used as proof of valid transactions. Each node has a copy of the ledger which makes it more transparent.
2. **Directed Acyclic Graphs (DAG):** This uses a different data structure to organize the data that brings more consensus. In this type of DLT, validation of transactions mostly requires the majority of support from the nodes in the network. Every node on the network has to provide proof of transactions on the ledger and then can initiate transactions. In this nodes have to verify at least two of the previous transactions on the ledger to confirm their transaction.
3. **Hash graph:** In this type of DLT, records are stored in the form of a directed acyclic graph. It uses a different consensus mechanism, using virtual voting as the form consensus mechanism for gaining network consensus. Hence nodes do not have to validate each transaction on the network.
4. **Holochain:** Holochain is termed as the next level of blockchain by some people because it is much more decentralized than blockchain. It is a type of DLT that simply proposes that each node will run on a chain of its own. Therefore nodes or miners have the freedom to operate autonomously. It basically moves to the agent-centric structure. Here agent means computer, node, miner,etc.
5. **Tempo or Radix:** Tempo uses the method of making a partition of the ledger this is termed sharding and then all the events that happened in the network are ordered properly. Basically, transactions are added to the ledger on basis of the order of events than the timestamp.



Advantages Of Distributed Ledger Technology

1. **High Transparency:** Distributed ledger presents a high level of transparency because all the transaction records are visible to everyone. The addition of data needs to be validated by nodes by using various consensus mechanisms. and if anyone tries to alter or change data in the ledger then it is immediately reflected across all nodes of the network which prevents invalid transactions.
2. **Decentralized:** In a centralized network, there may be a single point of failure and it can disrupt the whole network because of mistakes at the central authority level. But in the case of distributed networks, there is no risk of a single point of failure. because of the decentralized structure trust factor also increases in participating nodes. This decentralized nature of validation reduces the cost of transactions drastically.
3. **Time Efficient:** As this network is decentralized so there is no need for a central authority to validate transactions every time. Hence this time for validation of each transaction reduces drastically. In the case of DLT, transactions can be validated by members of the network itself by using various consensus mechanisms.
4. **Scalable:** Distributed ledger technology is more scalable because many different types of consensus mechanisms can be used to make it more reliant, fast, and updated. Because these many advanced DLT technologies are introduced in the last few years. Such as Holochain, hashgraph are considered to be advanced and more secure versions of Blockchain DLT. Blockchain itself is advanced and secure but DLT provides a way to more advanced technologies.

Uses of Distributed Ledger Technology

Because of all these benefits of distributed ledger technology and this technology has the potential to revolutionize many sectors like Financial, energy, healthcare, governance, supply chain management, real estate, cloud computing, etc.

1. **Banking:** In the banking sector right now transfer of money can be both expensive and time-consuming. Also sending money overseas becomes even more complex due to exchange rates and other hidden fees included. Here DLT can provide a decentralized secure network that will help to reduce the time, complexity, and costs required to transfer money. This decentralized network will eliminate the need for third parties which makes this system more complex and time-consuming.
2. **Cyber Security:** Nowadays cyber security has been emerging as a big threat to governments, enterprises, and individual people also. So it is essential to find an effective solution to secure our data and privacy against unauthorized access. In DLT, all information is authorized and securely encrypted by various cryptographic algorithms. This provides a transparent and secure environment and none of the data can be tempered by any entity.
3. **Supply chain management:** Supply chain is one of the complex structures itself. In this structure, it is hard to trace where the fault happened. So here Distributed ledger technology comes into the picture, Using DLT, you can easily trace the supply chain from the beginning to the end and can easily find out where a mistake or fault has happened. All the data added to the DLT is validated and permanent and can not be altered. This transparency of data enables us to trace from the beginning to the end of the ledger.
4. **Healthcare:** Distributed Ledger eliminates central authority and ensures rapid access to secured and untempered data. Here important medical can be stored securely and no one can change this data, even if someone tries to change it will be reflected everyone immediately. DLT can be used in the insurance sector to trace false claims because of its decentralized system.
5. **Governance:** DLT can be used in the government system to make it transparent among citizens. Many governments have adopted blockchain in the governance system because of the robustness of this system. It can be used as a voting system too. The traditional voting system has many flaws and sometimes it is found that there are many false voting and illegal activities that happen during voting. Online voting systems can be used to vote and with security and fake votes can be easily checked. everyone will have their own identity. So that any person sitting anywhere in the world can cast his vote.

How are Blockchain And Distributed Ledger Different?

In general blockchain and Distributed Ledger Technology are considered as same, but there are some differences between these two technologies. Blockchain can be

classified as a type of Distributed Ledger Technology. We can say that Blockchain is a type of DLT, but every Distributed Ledger can not be called a blockchain.

Blockchain is the parent technology of DLT. But the idea behind them is the same. Blockchain technology has the potential to solve many problems in the banking and financial industry. Here, blockchain is the advanced version of Distributed Ledger Technology with many useful functionalities. Developers have many other variants of DLTs in the technology world. However, they do not have the many real-life implementations and applications that blockchain has been able to do.

Basis	Distributed Ledger	Blockchain Technology
Block Structure	In DLT, blocks can be organized in different forms.	In Blockchain, blocks are added in the form of a chain.
Power of Work	It is more scalable because it does not need the power of a work consensus mechanism for the validation of each transaction.	It is a subset of DLT, the power of the work consensus mechanism adds more functionalities and security.
Tokens	It does not require any tokens or digital currency.	In it, tokens must be considered while working with Blockchain.
Sequence	It does not require any specific sequence of data.	All blocks are arranged in a particular series.
Trustability	Trust among participating nodes is high.	Trust among participating nodes is less than DLT. Decision-making powers can be on one hand because everyone can mine.

Advantages of Using Distributed Ledger Technology In Blockchain

1. **Security:** All records of every transaction are securely encrypted. Once the transaction is validated, it is completely secure and no one can update or change it. It is a permanent process.
2. **Decentralization:** All network members or nodes have a copy of the ledger for complete transparency. A decentralized private distributed network improves the reliability of the system and gives assurance of continuous operations without

any interruption. It gives control of information and data in the hand of the user.

3. **Anonymity:** The identity of each participant is anonymous and does not possibly reveal their identity.
4. **Immutable:** Any validated transactions cannot be changed as they are irreversible.
5. **Transparency:** Distributed technologies offer a high level of transparency. Which is necessary for the sectors like finance, medical science, banking, etc.
6. **Speed:** Distributed Ledger Technology can handle large transactions faster than traditional methods.
7. **Smart Contracts:** Distributed Ledger Technology supports smart contracts which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts reduce the need for intermediaries and offer transparency and automation in the execution of the contract terms.
8. **Lower Costs:** Distributed Ledger Technology eliminates intermediaries and reduces the costs associated with intermediaries, which makes the system more cost-effective.
9. **Improved Efficiency:** Distributed Ledger Technology reduces the time and costs associated with traditional transaction methods. It offers faster settlement times, reduced paperwork, and increased efficiency.
10. **Auditing:** Distributed Ledger Technology makes auditing easier as every transaction is recorded and the ledger cannot be altered. This improves the transparency and accuracy of financial audits.
11. **Resilience:** Distributed Ledger Technology is more resilient than traditional databases as it is spread across multiple nodes. This means that even if one node goes down, the network can still function as the rest of the nodes can continue to validate transactions.
12. **Traceability:** Distributed Ledger Technology offers complete traceability of assets, from their creation to their current ownership. This improves accountability and reduces the risks of fraud and theft.

Disadvantages Of Distributed Ledger Technology

1. **51% Attack:** The 51% attack is a bit concerning part of this distributed ledger technology that is to be checked routinely.
2. **Costs of Transaction:** The connected nodes are expected to validate the transaction of a given Distributed Ledger Technology which gives high transaction cost as the other nodes are paid incentives to validate the transaction.

3. **Slow Transaction Speed:** The major disadvantage of this DLT is the slow speed of transactions as multiple nodes are attached to this network and it takes time to validate the transaction by all the other nodes.
4. **Scalability Issues:** Due to low speed and high transaction costs DLT faces very difficulties to expand on a large scale.
5. **Lack of Regulation:** As DLT is a decentralized technology, it operates outside the control of any centralized authority which can lead to a lack of regulation, making it difficult to hold accountable any wrongdoings or fraudulent activities on the network.
6. **Energy Consumption:** Distributed Ledger Technology requires a significant amount of energy to maintain the network and validate transactions, especially in the case of Proof of Work consensus mechanisms, which can lead to a negative impact on the environment.
7. **Complexity:** Implementing and managing Distributed Ledger Technology can be complex and requires a high level of technical expertise, which can be a barrier to entry for many organizations and individuals.
8. **Privacy Concerns:** While the anonymity of participants on the network is considered an advantage, it can also be a disadvantage as it can lead to privacy concerns and illicit activities on the network.
9. **Lack of Interoperability:** Different Distributed Ledger Technologies may use different protocols, which can lead to interoperability issues, making it difficult for different networks to communicate and transact with each other.

Future of Distributed Ledger Technology

1. Experts in this area promote DLT as a solution for many problems that are present on the internet and will drastically be able to solve all these problems. Distributed Ledger Technology is termed the "Internet of Value". Transactions and processes will occur in real-time with the help of the internet.
2. Distributed Ledger Technology has the potential to impact problems in financial or banking, cyber security, healthcare, government, data security, etc. sectors with effective solutions.
3. Enterprises and visionaries are now faced with the challenge of establishing networks of entities that together can take advantage of DLT to radically change how they share and keep records, and innovate where DLT can enable entirely new processes and business models.

The Basics about Cryptocurrency

Cryptocurrency comes under many names. You have probably read about some of the most popular types of cryptocurrencies such as Bitcoin, Litecoin, and Ethereum. Cryptocurrencies are increasingly popular alternatives for online payments. Before converting real dollars, euros, pounds, or other traditional currencies into ₿ (the symbol for Bitcoin, the most popular cryptocurrency), you should understand what cryptocurrencies are, what the risks are in using cryptocurrencies, and how to protect your investment.

What is cryptocurrency? A cryptocurrency is a digital currency, which is an alternative form of payment created using encryption algorithms. The use of encryption technologies means that cryptocurrencies function both as a currency and as a virtual accounting system. To use cryptocurrencies, you need a cryptocurrency wallet. These wallets can be software that is a cloud-based service or is stored on your computer or on your mobile device. The wallets are the tool through which you store your encryption keys that confirm your identity and link to your cryptocurrency.

What are the risks to using cryptocurrency? Cryptocurrencies are still relatively new, and the market for these digital currencies is very volatile. Since cryptocurrencies don't need banks or any other third party to regulate them; they tend to be uninsured and are hard to convert into a form of tangible currency (such as US dollars or euros.) In addition, since cryptocurrencies are technology-based intangible assets, they can be hacked like any other intangible technology asset. Finally, since you store your cryptocurrencies in a digital wallet, if you lose your wallet (or access to it or to wallet backups), you have lost your entire cryptocurrency investment.

Follow these tips to protect your cryptocurrencies:

- Look before you leap! Before investing in a cryptocurrency, be sure you understand how it works, where it can be used, and how to exchange it. Read the webpages for the currency itself (such as Ethereum, Bitcoin or Litecoin) so that you fully understand how it works, and read independent articles on the cryptocurrencies you are considering as well.
- Use a trustworthy wallet. It is going to take some research on your part to choose the right wallet for your needs. If you choose to manage your cryptocurrency wallet with a local application on your computer or mobile device, then you will need to protect this wallet at a level consistent with your investment. Just like you wouldn't carry a million dollars around in a paper bag, don't choose an unknown or lesser-known wallet to protect your cryptocurrency. You want to make sure that you use a trustworthy wallet.
- Have a backup strategy. Think about what happens if your computer or mobile device (or wherever you store your wallet) is lost or stolen or if you don't otherwise have access to it. Without a backup strategy, you will have no way of getting your cryptocurrency back, and you could lose your investment.

What is Web 1.0, Web 2.0, and Web 3.0?
Definitions, Differences & Similarities

By John Terra

The digital age comes with its own lexicon, a bewildering array of buzz phrases, words, and acronyms designed to confuse as much as they are to inform. Many of these new terms have found their way into our everyday vocabularies, although the meanings often get confused and blurred.

For instance, many people use "the Web" and "the Internet" interchangeably when they are, in fact, two different things. Furthermore, there's more than one version of the Web. Are you intrigued yet?

This article will help you differentiate between Web 1.0, 2.0, and 3.0. It provides a Web 1.0 definition, Web 2.0 definition, Web 3.0 definition, Web 1.0 2.0 3.0 examples, and comparisons such as Web 1.0 vs. Web 2.0.

So, let's look at three different versions of this crucial online resource.

Oh, and incidentally, here's the difference between the Web and the Internet. The Web, formerly referred to as the World Wide Web, is the pages/sites you see when you log online. The Internet is a series of interconnected computer systems the Web functions on, plus the medium allows files and e-mails to travel along.

Or put another way, the Internet is the highway system that connects many cities, and the Web is the collection of rest stops, gas stations, convenience stores, and other stops. All versions of the Web have used and continue to use the Internet to connect users with websites and each other. That characteristic remains a constant.

Also, as an aside, no one really uses the term "World Wide Web" anymore. We still have a remnant of the phrase, though, because most URLs begin with the letters "www," which unsurprisingly stand for "World Wide Web." It's an indelible part of our Internet culture!

Okay, on with the different Web versions. What are the differences between Web 1.0, Web 2.0, and Web 3.0, and what are their similarities?

What Is Web 1.0?

Basically, this first version of the Web consisted of a few people creating web pages and content and web pages for a large group of readers, allowing them to access facts, information, and content from the sources.

Or you can sum up Web 1.0 like this: it was designed to help people better find information. This web version dealt was dedicated to users searching for data. This web version is sometimes called "the read-only Web" because it lacks the necessary forms, visuals, controls, and interactivity we enjoy on today's Internet.

People use the term "Web 1.0" to describe the earliest form of the Internet. Users saw the first example of a worldwide network that hinted at future digital communication and information-sharing potential.

Here are a few characteristics found in Web 1.0:

- It's made up of static pages connected to a system via hyperlinks
- It has HTML 3.2 elements like frames and tables
- HTML forms get sent through e-mail
- The content comes from the server's filesystem, not a relational database management system
- It features GIF buttons and graphics

Take a real-world dictionary, digitize everything in it, and make it accessible to people online to look at (but not be able to react to it). Boom. That's Web 1.0.

What Is Web 2.0?

If Web 1.0 was made up of a small number of people generating content for a larger audience, then Web 2.0 is many people creating even more content for a growing audience. Web 1.0 focused on reading; Web 2.0 focused on participating and contributing.

This Internet form emphasizes User-Generated Content (UGC), ease of use, interactivity, and improved compatibility with other systems and devices. Web 2.0 is all about the end user's experience. Consequently, this Web form was responsible for creating communities, collaborations, dialogue, and social media. As a result, Web 2.0 is considered the primary form of web interaction for most of today's users.

If Web 1.0 was called "the read-only Web," Web 2.0 is known as "the participative social Web." Web 2.0 is a better, more enhanced version of its predecessor, incorporating web browser technologies such as JavaScript frameworks.

Here's a breakdown of typical Web 2.0 characteristics:

- It offers free information sorting, allowing users to retrieve and classify data collectively
- It contains dynamic content that responds to the user's input
- It employs Developed Application Programming Interfaces (API)
- It encourages self-usage and allows forms of interaction like:
    - Podcasting
    - Social media
    - Tagging
    - Blogging

    - Commenting
    - Curating with RSS
    - Social networking
    - Web content voting
- It's used by society at large and not limited to specific communities.

Mobile Internet access and the rise of social networks have contributed to a dramatic upturn in Web 2.0's growth. This explosion is also fueled by the rampant popularity of mobile devices such as Android-powered devices and iPhones. In addition, Web 2.0's growth made it possible for apps such as TikTok, Twitter, and YouTube to expand and dominate the online landscape.

You're using Web 2.0 at this exact moment, you know.

What Is Web 3.0?

And finally, we come to the latest Web iteration.

When trying to figure out the definitive web 3.0 meaning, we need to look into the future. Although there are elements of Web 3.0 currently available today, it still has a way to go before it reaches full realization.

Web 3.0, which is also referred to as Web3, is built on a foundation consisting of the core ideas of decentralization, openness, and more excellent user utility. Web 1.0 is the "read-only Web," Web 2.0 is the "participative social Web," and Web 3.0 is the "read, write, execute Web."

This Web interaction and utilization stage moves users away from centralized platforms like Facebook, Google, or Twitter and towards decentralized, nearly anonymous platforms. World Wide Web inventor Tim Berners-Lee initially called Web 3.0 the Semantic Web and envisioned an intelligent, autonomous, and open Internet that used Artificial Intelligence and Machine Learning to act as a "global brain" and process content conceptually and contextually.

This idealized version didn't quite pan out due to technological limitations, like how expensive and complicated it is to convert human language into something readily understood by computers.

Here's a list of typical Web 3.0 characteristics:

- It's a semantic web, where the web technology evolves into a tool that lets users create, share, and connect content via search and analysis. It is based on comprehension of words instead of numbers and keywords.
- It incorporates Artificial Intelligence and Machine Learning. If these concepts are combined with Natural Language Processing (NLP), the result is a computer that uses Web 3.0 to become smarter and more responsive to user needs.
- It presents the connectivity of multiple devices and applications through the Internet of Things (IoT). Semantic metadata makes this process possible,

allowing all available information to be effectively leveraged. In addition, people can connect to the Internet anytime, anywhere, without needing a computer or smart device.

- It offers users the freedom to interact publicly or privately without having an intermediary expose them to risks, therefore offering people "trust less" data.
- It uses 3-D graphics. In fact, we already see this in computer games, virtual tours, and e-commerce.
- It facilitates participation without needing authorization from a governing body. It's permissionless.
- **It can be used for:**
    - Metaverses: A 3D-rendered, boundless, virtual world
    - Blockchain games: They allow users to have actual ownership of in-game resources, following the principles of NFTs
    - Privacy and digital infrastructure: This use includes zero-knowledge proofs and more secure personal information
    - Decentralized finance. This use includes payment Blockchains, peer-to-peer digital financial transactions, smart contracts, and cryptocurrency
    - Decentralized autonomous organizations. Community members own online communities

Web 3.0 ultimately lets users interact, exchange information, and securely conduct financial transactions without a centralized authority or coordinator. As a result, each user becomes a content owner instead of just a content user.

Remember that Web 3.0 isn't entirely in place. However, we are already seeing elements of Web 3.0 working their way into our Internet experiences, such as NFTs, Blockchain, Distributed ledgers, and the AR cloud. Additionally, Siri is Web 3.0 technology, as is the Internet of Things. However, if and when the full implementation happens, it will be closer to Berners-Lee's initial vision of Web 3.0. As he puts it, it will be a place with "no permission is needed from a central authority to post anything ... there is no central controlling node, and so no single point of failure ... and no "kill switch."

Unfortunately, there is still a lot of work to be done, especially in speech recognition; human speech has a staggering variety of nuances and terms that technology can't fully comprehend. There have been advances, but the process hasn't yet been perfected.

Uses of Web 1.0, Web 2.0, Web 3.0

- Uses of Web 1.0: Web 1.0 functions as a CDN (content delivery network), allowing a chunk of the website to be displayed on the website. As a result, it can be used as a personal website. The users would be charged in terms of each page view. It is made up of directories that allow its users to get a certain collection of information.

- Uses of Web 2.0: The social web comprises numerous platforms and tools. People contribute their opinions, insights, experiences, and thoughts on these sites. Thus, Web 2.0 tends to interact substantially more with its end users. These end users are not only the users of the programmes, but also the participants/viewers generated by podcasts, tagging, blogging, RSS curation, Web content voting, Social media, Social networking, Social bookmarking, and many more.
- Uses of Web 3.0: Web 3.0 are enhanced variations of the original Web 1.0 from the 1990s and early 2000s. Web 3.0 is the next generation of the current web that we are familiar with.

Potential and Pitfalls of Web 3.0

Potentials

1. Data ownership. You will have the choice of what details you want to provide to companies and advertising agencies, and you will be able to make money off of it.
2. There are fewer middlemen.
3. Transparency - Every stakeholder will constantly be aware of the worth and business they are connected to.
4. The improvement of internet data connections will be made possible via the semantic web.

Pitfalls

1. Users will need a device with above-average hardware to access Web3.
2. For newbies, it could be a little challenging to understand.
3. Difficult to regulate.
4. Simple access to users' private and open data

What Are the Differences Between the Web 1.0, Web 2.0, and Web 3.0?

Let's break down and examine the differences between the three Webs using this handy table.

Web 1.0	Web 2.0	Web 3.0
Typically read-only	Strongly read-write	Read-write-interact
Owned content	Shared content	Consolidated content

Visual/interactive Web	Programmable Web	Linked data Web
Home pages	Wikis and blogs	Waves and live streams
Web page	Web service endpoint	Data space
HTML/HTTP/URL/Portals	XML/RSS	RDF/RDFS/OWL
Page views	Cost per click	User engagement
File/web servers, search engines, e-mail, P2P file sharing, content and enterprise portals	Instant messaging, Ajax and JavaScript frameworks, Adobe Flex	Personal intelligent data assistants, ontologies, knowledge bases, semantic search functions
Directories	Tagging the user	User behaviour
Focus on the company	Focus on the community	Focus on the individual
Encyclopaedia Britannica online	Wikipedia	The Semantic Web
Banner advertising	Interactive advertising	Behavioural advertising
Active 1989-2005	Active 1999-2012	Active 2006-ongoing

Incidentally, just as the age range of various generations differs depending on who you get the information from (things like boomers, Generation X, and millennials), there's

also variance in Web version activity. For example, some sources classify Web 1.0 as 1990-2000, Web 2.0 as 2000-2010, and Web 3.0 as 2010-onward.

We can also say that Web 1.0 helped people find things online better, Web 2.0 enabled people to experience things better, and Web 3.0 helped people create things online better.

What Are the Similarities Between the Web 1.0, Web 2.0, and Web 3.0?

If you take a good look at all three different web versions, you notice that they only have a few fundamental traits in common. They are:

- They all deal with the relationship between end-users and information
- They all provide users with an iteration of the "read" function
- They all rely on the Internet to expedite their tasks

What Are Smart Contracts? Types, Benefits, and Tools

- A smart contract is defined as a digital agreement that is signed and stored on a blockchain network, which executes automatically when the contract's terms and conditions (T&C) are met. The T&C is written in blockchain-specific programming languages such as Solidity.
- Smart contracts form the foundation of most blockchain use cases, from non-fungible tokens (NFTs) to decentralized apps and the metaverse.
- This article explains how smart contracts work and details their various types. It also lists the top smart contract tools available and the best practices that need to be followed.

What Are Smart Contracts?

A smart contract is a digital agreement signed and stored on a blockchain network that executes automatically when the contract's terms and conditions (T&C) are met; the T&C is written in blockchain-specific programming languages like Solidity.

One can also look at smart contracts as blockchain applications that enable all parties to carry out their part of a transaction. Apps powered by smart contracts are frequently referred to as "decentralized applications" or "dapps."

While the idea of blockchain is largely perceived as Bitcoin's underlying tech driver, it has, since then, grown into a force to reckon with. Using smart contracts, a manufacturer requiring raw materials can establish payments, and the supplier can schedule shipments. Then, based on the contract between the two organizations, payments can be automatically transferred to the seller upon dispatch or delivery.

History of Smart Contracts

Nick Szabo, a U.S.-born computer scientist who developed a virtual currency dubbed "Bit Gold" in 1998, a decade before Bitcoin was introduced, was the first to propose smart contracts in 1994. Szabo characterized smart contracts as digital transaction mechanisms that implement a contract's terms.

Many predictions made by Szabo in his paper are now a part of our daily lives in ways that precede blockchain technology. However, this idea couldn't be implemented because the necessary technology, primarily the distributed ledger, did not exist then.

In 2008, Satoshi Nakamoto introduced the revolutionary blockchain technology in a whitepaper. It prevented transactions from being specified in another block. However, the emergence of cutting-edge technologies acted as stimuli for the rise of smart contracts. Five years on, the Ethereum blockchain platform made practical use of smart contracts achievable. Ethereum is still one of the most prevalent platforms enabling smart contract implementation.

How Do Smart Contracts Work?

Like any other contract, a smart contract is a binding contract between two parties. It uses code to take advantage of the advantages of blockchain technology, thereby

unlocking greater efficacy, openness, and confidentiality. The execution of smart contracts is controlled by relatively easy "if/when...then..." statements written in code on the blockchain.

These are the steps needed for the functioning of smart contracts.

- **Agreement:** The parties wanting to conduct business or exchange products or services must concur on the arrangement's terms and conditions. Furthermore, they must determine how a smart contract will operate, including the criteria that must be fulfilled for the agreement to be fulfilled.
- **Contract creation:** Participants in a transaction may create a smart contract in many ways, including building it themselves or collaborating with a smart contract provider. The provisions of the contract are coded in a programming language. During this stage, verifying the contract's security thoroughly is critical.
- **Deployment:** When the contract has been finalized, it must be published on the blockchain. The smart contract is uploaded to the blockchain in the same way as regular crypto transactions, with the code inserted into the data field of the exchange. Once the transaction has been verified, it's deemed active on the blockchain and cannot be reversed or amended.
- **Monitoring conditions:** A smart contract runs by tracking the blockchain or a different reliable source for predetermined conditions or prompts. These triggers can be just about anything that can be digitally verified, like a date attained, a payment made, etc.
- **Execution:** When the trigger parameters are met, the smart contract is activated as per the "if/when...then..." statement. This may implement only one or multiple actions, like passing funds to a vendor or registering the buyer's possession of an asset.
- **Recording:** Contract execution results are promptly published on the blockchain. The blockchain system verifies the actions taken, logs their completion as an exchange, and stores the concluded agreement on the blockchain. This document is available at all times.

Types of Smart Contracts

When it comes to the types of smart contracts, they are classified into three categories — legal contracts, decentralized autonomous organizations or DAOs, and logic contracts. Here, we'll discuss each of the three in more detail.

1. Smart legal contract

Smart contracts are guaranteed by law. They adhere to the structure of legal contracts: "If this happens, and then this will happen." As smart contracts reside on blockchain and are unchangeable, judicial or legal smart contracts offer greater transparency than traditional documents among contracting entities.

The parties involved execute contracts with digital signatures. Smart legal contracts may be executed autonomously if certain prerequisites are fulfilled, for example, making a payment when a specific deadline is reached. In the event of failure to comply, stakeholders could face severe legal repercussions.

2. Decentralized autonomous organizations

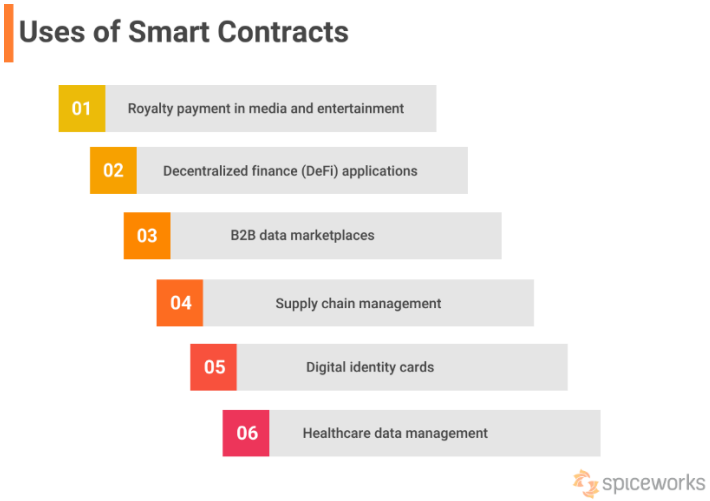
DAOs are democratic groups governed by a smart contract that confers them with voting rights. A DAO serves as a blockchain-governed organization with a shared objective that is collectively controlled. No executive or president exists. Instead, blockchain-based tenets embedded within the contract's code regulate how the organization functions and funds are allocated. VitaDAO is an example of this type of smart contract, where the technology powers a community for scientific research.

3. Application logic contracts

ALCs, or application logic contracts, consist of application-based code that typically remains synced with various other blockchain contracts. It enables interactions between various devices, like the Internet of Things (IoT) or blockchain integration. Unlike the other types of smart contracts, these are not signed between humans or organizations but between machines and other contracts.

Top 10 Uses of Smart Contracts

The uses of smart contracts are wide and varied, spread across industries.



Smart Contracts Uses

1. Royalty payment in media and entertainment

As they enter the industry, new artists rely on revenues from streaming services. Smart contract apps can facilitate easier royalty payments. These contracts can outline, for instance, the share of royalties payable to the record company and the artist. Instantaneous handling of these payments is an enormous advantage for everyone involved.

Smart contracts could also potentially solve the challenge of royalty distribution in an over-the-top (OTT) content world where traditional network agreements do not apply.

This technology allows emerging artists and lesser-known actors to get small but regular payments.

2. Decentralized finance (DeFi) applications

Using cryptocurrencies and smart contracts, DeFi apps can offer financial services without an intermediary. DeFi is no longer limited to peer-to-peer transactions. On DeFi platforms, smart contracts facilitate complex processes like borrowing, lending, or derivative transactions.

3. Conversion of assets into non-fungible tokens (NFTs)

By assigning ownership and administering the movable nature of digital assets, smart contracts have made it possible to create non-fungible tokens (NFTs). Contracts like this can also be altered to include added stipulations, like royalties, along with access rights to platforms or software. Essentially, smart contracts make it possible to treat digital assets just like physical ones, with real tangible value.

4. B2B data marketplaces

A data marketplace is a portal where users can buy and sell diverse datasets or data streams from a wide range of sources. Intelligent contracts facilitate the creation of dynamic and fast-evolving markets that support automated and secure transactions without the hassle of human intervention. Datapace is a good example of this particular smart contract use case.

5. Supply chain management

Smart contracts may work autonomously without mediators or third parties because they are self-executing. An organization can create smart contracts for an entire supply chain. This would not require regular management or auditing. Any shipments received beyond the schedule might trigger stipulated escalation measures to guarantee seamless execution.

6. Digital identity cards

Users can store reputational data and digital assets on smart contracts to generate a digital identification card. When smart contracts are linked to multiple online services, other external stakeholders can learn about individuals without divulging their true identities.

For instance, these contracts may include credit scores lenders can use to verify loan applicants without the risk of demographic profiling or discrimination. Similarly, candidates can share resumes without the risk of gender bias in hiring.

7. Electoral polls

Voting could occur within a secure environment created by smart contracts, minimizing the likelihood of voter manipulation. Due to the encryption, every vote is ledger-protected and extremely difficult to decode. Additionally, smart contracts might boost voter turnout. With an online voting system driven by smart contracts, one can avoid making trips to a polling location.

8. Real estate

Smart contracts can accelerate the handover of property ownership. Contracts can be autonomously created and executed. After the buyer's payment to the vendor, for instance, the smart contract may immediately assign control over the asset dependent on the blockchain's payment record.

9. Healthcare data management

Smart contracts can revolutionize healthcare by making data recording more open and efficient. For instance, they might encourage clinical trials by guaranteeing data integrity. Hospitals can maintain accurate patient data records and effectively manage appointments.

10. Civil law

Smart contracts can also flourish in the legal industry. It can be used to create legally binding business and social contracts. In certain regions of North America, governments have authorized smart contracts for digitized agreements. For example, California can issue marital and birth certificates as smart contracts.

Benefits and Challenges of Smart Contracts

Like any technology, smart contracts have both pros and cons. Here are the benefits of smart contracts first:

Benefits of smart contracts

The key reasons to use smart contracts include:

1. Single source of truth

Individuals have the same data at all times, which reduces the likelihood of contract clause exploitation. This enhances trust and safety because contract-related information is accessible throughout the duration of the contract. Additionally, transactions are replicated so that all involved parties have a copy.

2. Reduction in human effort

Smart contracts don't need third-party verification or human oversight. This provides participants autonomy and independence, particularly in the case of DAO. This intrinsic characteristic of smart contracts offers additional benefits, including cost savings and faster processes.

3. Prevention of errors

A fundamental prerequisite for any contract is that every term and condition is recorded in explicit detail. An omission may result in serious issues in the future, including disproportionate penalties and legal complexities. Automated smart contracts avoid form-filling errors. This is one of its greatest advantages.

4. Zero-trust by default

The entire framework of smart contracts is a step beyond conventional mechanisms. This implies that there's no need to rely on the trustworthy conduct of other parties during a transaction. A transaction or exchange does not necessitate faith as a fundamental component, consistent with zero-trust security standards. Since smart contracts operate on a decentralized network, every aspect of the network is more open, fair, and equitable, with no risk of privilege creep.

5. Built-in backup

These contracts capture essential transactional details. Therefore, whenever your data is used in a contract, it is stored indefinitely for future reference. In an instance of data loss, it is simple to retrieve these properties.

Challenges of smart contracts

Here are the potential downsides of smart contracts and the challenges to be aware of:

1. Rigidity and inconsistent support

Modifying smart contract protocols is nearly impossible, and fixing code errors can be costly and time-consuming. Even if smart contracts conform to the laws of different countries, it might be tough to guarantee that they are adhered to globally.

2. Difficulty in capturing unquantifiable data

For businesses with quantifiable data, such as finance and agriculture, it is relatively simple to put together smart contracts. However, not all industries use quantifiable metrics, like scenarios where creative work has to be evaluated.

3. Conflict with GDPR

The General Data Protection Regulation (GDPR) guarantees *the right to be forgotten by its citizens.* They can request that digital data about them be deleted. Nevertheless, if a digital legal contract binds an individual, it cannot be erased or redacted.

4. Skills shortage

The creation of smart contracts demands expertise in software engineering. Smart contract development is distinct from traditional software development in that it requires coders with organizational expertise and comprehension of non-traditional programming languages such as Solidity. These skills are hard to come by.

5. Scalability Issues

Finally, there is the question of magnitude and scale. Visa can currently process approximately 24,000 transactions per second. According to Worldcoin's 2023 update, Ethereum, the world's biggest blockchain for smart contracts, can only manage 30 transactions per second.

Top Smart Contract Tools

Some of the top tools meant for smart contract developers are:

1. BoringSolidity

BoringSolidity is a collection of libraries for developing Solidity smart contracts that aim to streamline and standardize routine tasks, minimize weaknesses, and enhance overall code quality. ConsenSys Diligence, a prominent security auditing company in the blockchain industry, created it.

2. Chainlink

Oracles on the blockchain aggregate real-world data from various sources and transfer it to smart contracts using the blockchain. Chainlink is among the leading Oracle solutions accessible today. It provides reliable and tamper-resistant data to support smart contracts throughout multiple blockchains.

3. Ethcode

Ethcode acts as a Visual Studio Code extension for developing Ethereum smart contracts. It provides a beginner-friendly development environment for text, troubleshooting, or unit testing contractual code. The code being used is open-source and simple for Microsoft users to use.

4. Octopus

Octopus is a tool to perform an in-depth evaluation of smart contract source code. It offers features for evaluating code, like symbolic execution, call flow analysis or control flow analysis. This will enable you to detect and correct contract errors before it's too late.

5. OpenZeppelin

OpenZeppelin has become among the most prominent no-code tools employed in smart contracts. This open-source framework offers a library of easily-integrated, safe, community-reviewed smart contracts. It also provides audit and authentication services for smart contracts.

6. Solidity

Solidity is the primary language used to create smart contracts in the Ethereum blockchain. When it comes to the user interface, it mirrors Python, C++, and JavaScript. As they are consistent with the Ethereum Virtual Machine (EVM), Solidity applications may run on other blockchains, like Polygon and Avalanche.

Best Practices for Using Smart Contracts

When working with smart contracts, one should remember the following best practices:

1. Prioritize simplicity

Incorporating a smart contract into an agreement adds value and unleashes blockchain's many advantages. Complex contract logic, on the other hand, can lead to errors or wasted time. Consequently, developing simple contract logic to implement optimal digital processes is vital. It is prudent to use pre-written code as it reduces the possibility of execution errors.

2. Update contracts regularly

Staying on top of contracts allows you to identify errors or vulnerable spots that must be resolved. Additionally, safety checks and frequent upgrades to newer versions improve the user experience and safeguard transactions. Since there is no human intervention, updating smart contracts is especially important.

3. Lock compiler versions for smart contract code

Software developers frequently make the error of not securing a compiler version in contract codes. By explicitly mentioning the compiler versions, you guarantee your contracts operate consistently across environments, avoiding release and authentication challenges.

4. Conduct rigorous testing

Evaluating the contracts on the test network before deploying them on the mainnet is imperative. This should allow you to identify defects or malfunctions before they become a significant problem. This best practice is crucial since it is difficult to fix smart contracts once they go live.

5. Work with experts on independent audits

As smart contracts function on a decentralized and trustless network, the code must be trusted. A smart contract's flaws can be attacked, and the deposited funds can be misappropriated. Therefore, security auditing is essential.

What Is a Crypto Wallet?

What Is a Crypto Wallet?

Cryptocurrency wallets store users' public and private keys while providing an easy-to-use interface to manage crypto balances. They also support cryptocurrency transfers through the blockchain. Some wallets even allow users to perform certain actions with their crypto assets, such as buying and selling or interacting with decentralised applications (dapps).

It is important to remember that cryptocurrency transactions do not represent a 'sending' of crypto tokens from a person's mobile phone to someone else's mobile phone. When sending tokens, a user's private key signs the transaction and broadcasts it to the blockchain network. The network then includes the transaction to reflect the updated balance in both the sender's and recipient's address.

So, the term 'wallet' is somewhat of a misnomer, as crypto wallets don't actually store cryptocurrency in the same way physical wallets hold cash. Instead, they read the public ledger to show the balances in a user's addresses, as well as hold the private keys that enable the user to make transactions.

Not Sure What a Public or Private Key Is?

A key is a long string of random, unpredictable characters. While a **public key** is like a bank account number and can be shared widely, the **private key** is like a bank account password or PIN and should be kept secret. In public key cryptography, every public key is paired with one corresponding private key. Together, they are used to encrypt and decrypt data.

Why a Crypto Wallet Is Needed for Storing Crypto Assets

A user's cryptocurrency is only as safe as the method they use to store it. While crypto can technically be stored directly on an exchange, it is not advisable to do so unless in small amounts or with the intention of trading frequently.

For larger amounts, it's recommended that a user withdraws the majority to a crypto wallet, whether that be a hot wallet or a cold one. This way, they retain ownership of their private keys and have full power and control over their own finances.

How Do Cryptocurrency Wallets Work?

As mentioned earlier, a crypto wallet doesn't technically hold a user's coins. Instead, it holds the *key* to their coins, which are stored on public blockchain networks.

In order to perform various transactions, a user needs to verify their wallet address via a private key that comes in a set of specific codes. The speed and security often depend on the kind of wallet a user has.

Different Types of Crypto Wallets

There are two main types of cryptocurrency wallets: software-based hot wallets and physical cold wallets. Read on to learn about the different types of crypto wallets, and which may be a best fit.

Hot Wallets and Cold Wallets — What's the Difference?

Hot Wallets

The main difference between hot and cold wallets is whether they are connected to the internet. **Hot wallets are connected to the internet, while cold wallets are kept offline.** This means that funds stored in hot wallets are more accessible and, therefore, easier for hackers to gain access to.

Examples of hot wallets include:

- Web-based wallets
- Mobile wallets
- Desktop wallets
- Software wallets

In hot wallets, private keys are stored and encrypted on the app itself, which is kept online. Using a hot wallet can be risky since computer networks have hidden vulnerabilities that can be targeted by hackers or malware programmes to break into the system. Keeping large amounts of cryptocurrency in a hot wallet is a fundamentally poor security practise, but the risks can be mitigated by using a hot wallet with stronger encryption, or by using devices that store private keys in a secure enclave.

There are different reasons why a market participant might want their cryptocurrency holdings to be either connected to or disconnected from the internet. Because of this,

it's not uncommon for cryptocurrency holders to have multiple cryptocurrency wallets, including both hot and cold ones.

Cold Wallets

As introduced at the beginning of this section, a cold wallet is entirely offline. While not as convenient as hot wallets, cold wallets are far more secure. An example of a physical medium used for cold storage is a piece of paper or an engraved piece of metal.

Examples of cold wallets include:

- Paper wallets
- Hardware wallets

What Is a Paper Wallet?

A paper wallet is a physical location where the private and public keys are written down or printed. In many ways, this is safer than keeping funds in a hot wallet, since remote hackers have no way of accessing these keys, which are kept safe from phishing attacks. On the other hand, it opens up the potential risk of the piece of paper getting destroyed or lost, which may result in irrecoverable funds.

What Is a Hardware Wallet?

A hardware wallet is an external accessory (usually a USB or Bluetooth device) that stores a user's keys; a user can only sign a transaction by pushing a physical button on the device, which malicious actors cannot control.

The best practise to store cryptocurrency assets that do not require instant access is offline in a cold wallet. However, users should note this also means that **securing their assets is entirely their own responsibility** — it is up to them to ensure they don't lose the hardware wallet, or have it stolen.

Tip: For increased security, separate the public and private keys, keep them offline, and store the physical wallet in a safe deposit box.

Hot Wallets vs Cold Wallets: Which Are Better?

While both methods of storage have benefits and drawbacks, the option depends on a user's preference. For example:

- For day-to-day trading, accessibility is of paramount importance, meaning that a hot wallet may be worth researching.
- However, for those considering storing a large amount of crypto assets and who value security over convenience, then consider researching a cold wallet.

Custodial and Non-Custodial Crypto Wallets

In addition to those mentioned above, wallets can be further separated into custodial and non-custodial types.

CUSTODIAL	NON-CUSTODIAL
A custodian or third party has control of the private keys	Users have complete control of their private keys and funds
Less secure, as funds are stored online and therefore vulnerable to hacking	More secure, as users hold their private keys offline
Less personal responsibility but requires trust in the custodian that holds user funds	Users are wholly responsible for keeping their funds and private keys secure
Backups in place, so if users lose their private key, they can easily regain access to their wallet	If users lose their private keys or recovery passwords, then they lose access to their funds
Lengthy KYC and AML procedures	No KYC or AML procedures
More user-friendly	Less user-friendly
Best suited to beginners just starting out	Best suited to those who want to retain full control of their funds

Custodial Wallets

Most web-based crypto wallets, also known as hosted wallets, tend to be custodial wallets. Typically offered on cryptocurrency exchanges, these wallets are known for their convenience and ease of usage, and are especially popular with newcomers, as well as experienced day traders.

The main difference between custodial wallets and the types mentioned above is that users are **no longer in full control of their tokens,** and the private keys required to sign for transactions are held only by the exchange.

The implication here is that **users must trust the service provider to securely store their tokens and implement strong security measures to prevent unauthorised access.** These measures include two-factor authentication (2FA), email confirmation, and biometric authentication, such as facial recognition or fingerprint verification. Many exchanges will not allow a user to make transactions until these security measures are properly set up.

Crypto exchanges and custodial wallet providers usually also take further steps to ensure the safety of users' tokens. For example, a portion of the funds is generally transferred to the company's cold wallet, safe from online attackers.

Crypto.com has taken many measures to ensure the protection of customer funds. After rigorous security audits by a team of cybersecurity and compliance experts, Crypto.com is the first crypto company in the world to have obtained ISO/IEC 27701:2019, ISO22301:2019, ISO27001:2013, and PCI: DSS 3.2.1, Level 1 compliance, and

independently assessed at Tier 4, the highest level for both NIST Cybersecurity and Privacy Frameworks, as well as Service Organization Control (SOC) 2 compliance.

Additionally, the company has in place a total of US$150 million for insurance protection of customer funds.

Non-Custodial Wallets

Non-custodial wallets, on the other hand, allow a user to retain full control of their funds, since the private key is stored locally with the user.

When starting a non-custodial wallet, the user is asked to write down and safely store a list of 12 randomly generated words, known as a 'recovery', 'seed', or 'mnemonic' phrase. From this phrase, the user's public and private keys can be generated. This acts as a **backup or recovery mechanism** in case the user loses access to their device.

Anyone with the seed phrase is able to gain full control of the funds held in that wallet. In a case scenario where the seed phrase is lost, the user also loses access to their funds. So it is imperative to keep the mnemonic phrase in a secure location, and to not store a digital copy of it anywhere. Do not print it out at a public printer or take a picture of it.

Note that hardware wallets are inherently non-custodial, since private keys are stored on the device itself. There are also software-based non-custodial wallets, such as the Crypto.com DeFi Wallet. The common theme is that **the private keys and the funds are fully in the user's control.** As the popular saying within the crypto community goes, 'not your keys, not your coins!'.

On the flip side, this means that users must be in charge of their own security with regard to the storage of passwords and seed phrases. If any of these are lost, recovery can be difficult or impossible because they are typically not stored on any third-party server.

Custodial vs Non-Custodial Wallets: Which Are Better?

Custodial and non-custodial wallets have various pros and cons that make them suitable for different types of users. Ultimately, it all comes down to personal choice.

- For those prone to losing passwords and devices, then it makes sense to use a custodial wallet, since an exchange or custodian is likely to have better security practices and backup options. That's why it's a popular option for beginners who have little to no experience trading crypto. Further, transaction fees with a custodial wallet tend to be cheaper or even free.
- For those who prefer to retain full control over their own funds, consider a non-custodial wallet.

For more on the differences between custodial and non-custodial wallets, see our university article Custodial vs Non-Custodial Wallets.

For Additional Security, Consider Multi-Signature Wallets

Multi-signature wallets — or multisig wallets — require two or more private key signatures to authorise transactions. This solution is useful for a number of use cases:

- An individual using a multisig wallet can **prevent losing access to the entire wallet in a case scenario where one key is lost.** For example, if a user loses one key, there will still be two other keys able to sign transactions.
- Multisig wallets can prevent the misuse of funds and fraud, which makes them a **good option for hedge funds, exchanges, and corporations.** Since each authorised person has one key, and a sign-off requires the majority of keys, it becomes impossible for any individual to unilaterally make unauthorised transactions.

Any of the wallet types described above — hot wallets, cold wallets, hardware wallets, etc. — have multisig versions.

NFT Wallets

An NFT wallet is a secure place that stores non-fungible tokens (NFTs). For NFT wallets, there are two main choices: hardware wallets or software-based wallets.

What to Look for in an NFT Wallet

The right NFT wallet depends on a variety of factors, including a user's level of experience and security needs, as well as the types of tokens they plan on storing. Below are things to consider when choosing an NFT wallet:

- **Compatibility with NFT marketplaces** — Users need a crypto wallet that can integrate with the NFT marketplaces they want to buy from.
- **Strong security** — Includes two-factor authentication (2FA), email confirmation, or biometric authentication.
- **User-friendly interface** — A good NFT wallet should boast a streamlined user experience and be easy to set up.
- **Accessibility on multiple devices** — Most NFT wallets are available via web extensions or as mobile/desktop applications. For enhanced convenience, look for a wallet that's available on multiple devices that can also synchronise transactions in real time.
- **Cross-chain compatibility** — Most wallets support Ethereum-based tokens; however, for those who want to mint, buy, and sell tokens on other networks, a crypto wallet with cross-chain compatibility is needed.

For a popular all-in-one hardware wallet, consider the Crypto.com DeFi Wallet, widely regarded as one of the most trusted and secure wallets to store NFTs — and voted the best NFT wallet 2024 by TradingPlatforms.

More About Crypto.com DeFi Wallet

The Crypto.com DeFi Wallet is non-custodial, which means that users retain full control of their private keys and assets. Available on Android and iOS, DeFi Wallet allows

users to manage 700-plus tokens across 30-plus blockchains and send crypto to anyone at their preferred confirmation speed and network fee. Additionally, users can buy crypto directly through their credit or debit card with Crypto.com Pay.

The dedicated wallet supports NFTs on Ethereum, Cronos, and Crypto.org Chain, and enables users to easily view top collections using the NFT Spotlight feature. Users can also use the wallet to potentially earn passive income by locking up cryptocurrencies like CRO, USDC, and DOT. Crypto.com users can also manage their NFTs within the Crypto.com App.

Learn more about Crypto.com NFT.

Conclusion

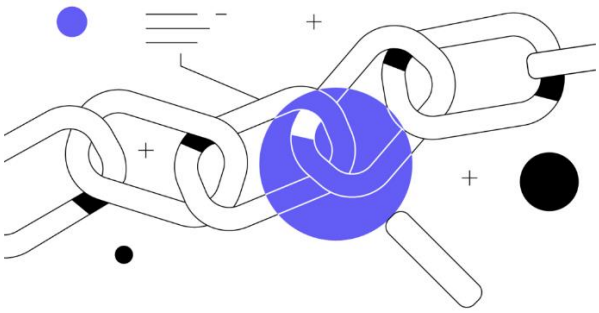
When it comes to crypto wallets, there is no perfect solution. Each type of wallet has different strengths, purposes, and trade-offs. It's up to the user to weigh what works best for them:

- For those with a high-risk tolerance who want to make regular, quick online payments, the convenience of a hot wallet, like the Crypto.com App, could suit best.
- For those a little more risk-averse who intend to hold their coins long term, then a secure offline device, like hardware wallets, might make the most sense.
- The final choice remains in the user's hands, with the non-custodial Crypto.com DeFi Wallet one of many secure options.

As storing large quantities of cryptocurrency in a single wallet is quite risky, **a combination of cold and hot wallets is usually ideal** and can help strike the right balance between convenience and security.

What Is a Block Explorer?

Block explorers enable you to search for information on a particular blockchain.



The Block Explorer: A Window into the Blockchain

Blockchain technology is often lauded for its transparency, and block explorers are a key part of this value proposition. A block explorer is an online tool that enables you to search for real-time and historical information about a blockchain, including data related to blocks, transactions, addresses, and more.

Every block explorer contains information about one particular blockchain — you cannot use a single explorer to retrieve information about Bitcoin and Ethereum; you'd need a Bitcoin block explorer and Ethereum block explorer, respectively. However, some sites host block explorers for multiple blockchains. Popular block explorer providers for Bitcoin and Ethereum include etherscan.io, blockstream.info, blockchain.com, and CoinMarketCap, among others.

Why Use a Block Explorer?

Block explorers have potential utility for traders, miners, validators, businesses, and enthusiasts alike. You can use a block explorer to check the status of a transaction if you're buying or selling crypto. You can also acquire information associated with your blockchain address, including your transaction history, the total value of the assets held at the address, the total amount of crypto received at the address, and the total amount of crypto sent from the address, among other data points.

Miners can use block explorers to check if they've successfully mined a block, and businesses can analyse transaction data related to their projects. Likewise, anyone can use block explorers to monitor the activity of whales and individuals with known blockchain addresses. For example, monitoring addresses known to belong to Satoshi Nakamoto is a favourite community pastime.

Block explorers also enable enthusiasts to find technical information about the inner workings of the blockchain, such as latest transactions and blocks, block difficulty, hash rate, block height, transaction fees, transaction volume, and more. Likewise, a block explorer can provide market data such as the circulating supply, maximum supply, and market capitalization of a cryptocurrency.

It is important to note that the information a block explorer contains may vary depending upon the architecture of the blockchain it serves. For example, a block

explorer for a Proof-of-Work (PoW) blockchain will display data about miners, whereas a block explorer for a Delegated Proof-of-Stake (DPoS) blockchain will display information about block producers and elections.

How to Use a Block Explorer

When you visit a block explorer site, you will likely see a main search bar that enables you to retrieve specific types of information — typically wallet addresses, transaction hashes, and block numbers, though this varies by explorer and by blockchain. Likewise, the homepage of most block explorers often displays data about the latest transactions and blocks.

To view data related to a particular transaction, type the transaction hash or ID into the search bar — this will be given to you by your wallet software when you initiate the transaction. The block explorer will indicate whether your transaction has been confirmed or if it is still processing. You can also view your transaction by searching for the address of the wallet you sent it from. Make sure that you enter your public key address and not your private key address when searching. Searching for your transaction by the block in which it was included is not recommended, as the block is likely to contain many other transactions.

It's perhaps helpful to conceptualize a block explorer like a search engine for a blockchain. These useful tools provide insight into every aspect of a blockchain's functioning — from consensus mechanism to transaction history — and are an essential tool in navigating the blockchain ecosystem.

Layer-1 and Layer-2 Blockchain Scaling Solutions

There are two primary ways to achieve blockchain scalability: Layer-1 and Layer-2 solutions.

What Is Blockchain Scalability?

While blockchain technology is proving itself to be a new pillar of the global economy, its underlying structure of decentralized networks faces a unique challenge known as the Blockchain Trilemma: the balancing act between decentralization, security, and scalability within a blockchain infrastructure.

Blockchain decentralization refers to the meaningful distribution of computing power and consensus throughout a network, while security reflects a blockchain protocol's defences against malicious actors and network attacks. Both are considered non-negotiable to the function of a blockchain network.

Also essential is scalability, which refers to a blockchain network's ability to support high transactional throughput and future growth. Scalability is crucial because it represents the only way for blockchain networks to reasonably compete with legacy, centralized platforms with rapid settlement times. A commonly used comparison to indicate the gulf in scalability is that Bitcoin processes between 4–7 transactions per second (TPS). Visa, on the other hand, processes thousands of TPS. In order to compete with these existing systems, blockchain technology must match or exceed these high levels of scalability. There now exists an entire sub-sector of the blockchain industry that's working towards improving scalability.

Thankfully, a whole new generation of blockchains and scaling solutions built specifically to solve this transaction-capacity problem is exponentially increasing the scaling limits of blockchain and making meaningful progress. These projects address scalability in two different ways: Layer-1 and Layer-2 scaling solutions.

Layer-1 Scaling Solutions

In the decentralized ecosystem, a Layer-1 network refers to a blockchain, while a Layer-2 protocol is a third-party integration that can be used in conjunction with a Layer-1 blockchain. Bitcoin, Litecoin, and Ethereum, for example, are Layer-1 blockchains. Layer-1 scaling solutions augment the base layer of the blockchain protocol itself in order to improve scalability. A number of methodologies are currently being developed — and practiced — that improve the scalability of blockchain networks directly.

Here's how it works: Layer-1 solutions change the rules of the protocol directly to increase transaction capacity and speed, while accommodating more users and data. Layer-1 scaling solutions can entail, for example, increasing the amount of data contained in each block, or accelerating the rate at which blocks are confirmed, so as to increase overall network throughput.

Other foundational updates to a blockchain to achieve Layer-1 network scaling include:

Consensus protocol improvements: Some consensus mechanisms are more efficient than others. Proof of Work (PoW) is the consensus protocol currently in use on popular blockchain networks like Bitcoin. Although PoW is secure, it can be slow. That's why many newer blockchain networks Favor the Proof-of-Stake (PoS) consensus mechanism. Instead of requiring miners to solve cryptographic algorithms using substantial computing power, PoS systems process and validate new blocks of transaction data based on participants staking collateral in the network.

With Ethereum 2.0, Ethereum will transition to a PoS consensus algorithm, which is expected to dramatically and fundamentally increase the capacity of the Ethereum network while increasing decentralization and preserving network security.

Sharding: Sharding is a mechanism adapted from distributed databases that has become one of the most popular Layer-1 scaling solutions, despite its somewhat experimental nature within the blockchain sector. Sharding entails breaking the state of the entire blockchain network into distinct datasets called "shards" — a more manageable task than requiring all nodes to maintain the entire network. These network shards are simultaneously processed in parallel by the network, allowing for sequential work on numerous transactions.

Further, each network node is assigned to a particular shard instead of maintaining a copy of the blockchain in its entirety. Individual shards provide proofs to the mainchain and interact with one another to share addresses, balances, and general states using cross-shard communication protocols. Ethereum 2.0 is one high-profile blockchain protocol that is exploring shards, along with Zilliqa, Tezos, and Qtum.

Layer-2 Scaling Solutions

Layer-2 refers to a network or technology that operates on top of an underlying blockchain protocol to improve its scalability and efficiency. This category of scaling solutions entails shifting a portion of a blockchain protocol's transactional burden to an adjacent system architecture, which then handles the brunt of the network's processing and only subsequently reports back to the main blockchain to finalize its results. By abstracting the majority of data processing to auxiliary architecture, the base layer blockchain becomes less congested — and ultimately more scalable.

For instance, Bitcoin is a Layer-1 network, and the Lightning Network is a Layer-2 solution built to improve transaction speeds in this fashion on the Bitcoin network. Other examples of Layer-2 solutions include:

Nested blockchains: A nested blockchain is essentially a blockchain within — or, rather, atop — another blockchain. The nested blockchain architecture typically involves a main blockchain that sets parameters for a broader network, while executions are undertaken on an interconnected web of secondary chains. Multiple blockchain levels can be built upon a mainchain, with each level using a parent-child connection. The parent chain delegates work to child chains that process and return it to the parent after completion. The underlying base blockchain does not take part in the network functions of secondary chains unless dispute resolution is necessary.

The distribution of work under this model reduces the processing burden on the mainchain to exponentially improve scalability. The OMG Plasma project is an example of Layer-2 nested blockchain infrastructure that is utilized atop the Layer-1 Ethereum protocol to facilitate faster and cheaper transactions.

State channels: A state channel facilitates two-way communication between a blockchain and off-chain transactional channels and improves overall transaction capacity and speed. A state channel does not require validation by nodes of the Layer-1 network. Instead, it is a network-adjacent resource that is sealed off by using a multi-signature or smart contract mechanism. When a transaction or batch of transactions is completed on a state channel, the final "state" of the "channel" and all its inherent transitions are recorded to the underlying blockchain. The Liquid Network, Celer, Bitcoin Lightning, and Ethereum's Raiden Network are examples of state channels. In the Blockchain Trilemma trade-off, state channels sacrifice some degree of decentralization to achieve greater scalability.

Sidechains: A sidechain is a blockchain-adjacent transactional chain that's typically used for large batch transactions. Sidechains use an independent consensus mechanism — i.e., separate from the original chain — which can be optimized for speed and scalability. With a sidechain architecture, the primary role of the mainchain is to maintain overall security, confirm batched transaction records, and resolve disputes. Sidechains are differentiated from state channels in a number of integral ways. Firstly, sidechain transactions aren't private between participants — they are publicly recorded to the ledger. Further, sidechain security breaches do not impact the mainchain or other sidechains. Establishing a sidechain might require substantial effort, as the infrastructure is usually built from the ground up.

Boosting Blockchain Network Scalability

Layer-1 and Layer-2 scaling solutions are two sides of the same crypto coin: They're strategies designed to make blockchain networks faster and more accommodating to a rapidly growing user base. These strategies are not mutually exclusive either, and many blockchain networks are exploring combinations of Layer-1 and Layer-2 scaling solutions to achieve increased scalability without sacrificing adequate security or decentralization.

What Is a Blockchain Oracle?

Last Updated Date:

January 12, 2024

Blockchain Oracle Definition

Blockchain oracles are entities that connect blockchains to external systems, thereby enabling smart contracts to execute based upon inputs and outputs from the real world.

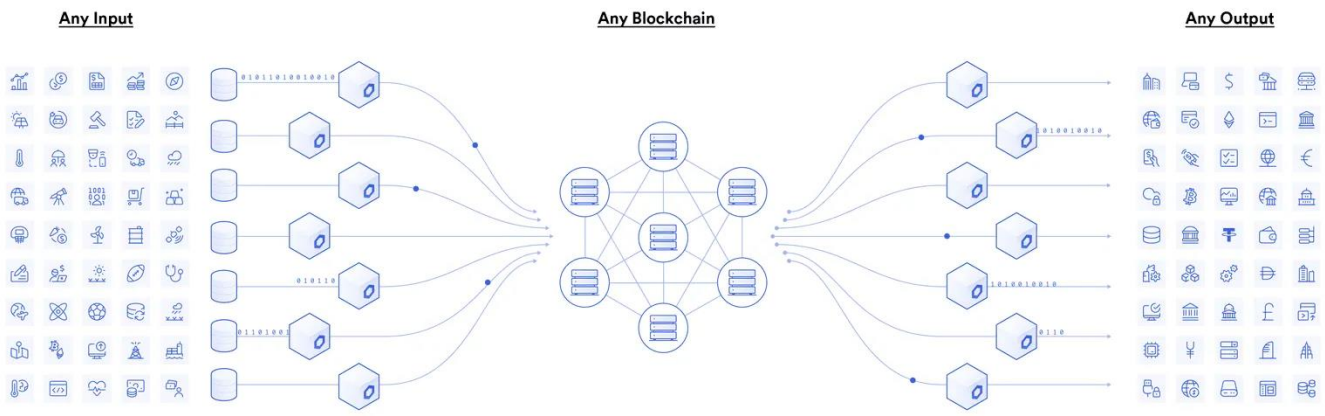
With the potential for hundreds of trillions of dollars worth of assets to move onchain, blockchain technology is transforming financial markets, global trade, insurance, gaming, and many other industries. Together, blockchains, smart contracts, and oracles underpin the verifiable web, where users can understand exactly what's going on within an application and remain in control of their assets at all times.

Oracles play a foundational role in the creation of the verifiable web, connecting blockchains that would otherwise be isolated to offchain data and compute, and enabling interoperability between blockchains. Initially, the Chainlink oracle network enabled the creation of the DeFi space and then grew to become the industry standard oracle solution for all of Web3. To date, Chainlink has enabled over $9T in transaction value. Now, Chainlink is collaborating with some of the world's largest financial institutions, including Swift, the global messaging network for 11K+ banks, DTCC, the world's largest securities settlement system processing $2+ quadrillion annually, and Australia and New Zealand Banking Group Limited (ANZ), a leading institution bank with $1T+ in AUM.

With an entire suite of services that enable developers to build advanced, secure, cross-chain, and verifiable applications, the Chainlink platform is set to help scale blockchain technology to billions of users.

What Is an Oracle Network?

Oracles provide a way for the decentralized Web3 ecosystem to access existing data sources, legacy systems, and advanced computations. Decentralized oracle networks (DONs) enable the creation of hybrid smart contracts, where onchain code and offchain infrastructure are combined to support advanced decentralized applications (dApps) that react to real-world events and interoperate with traditional systems.

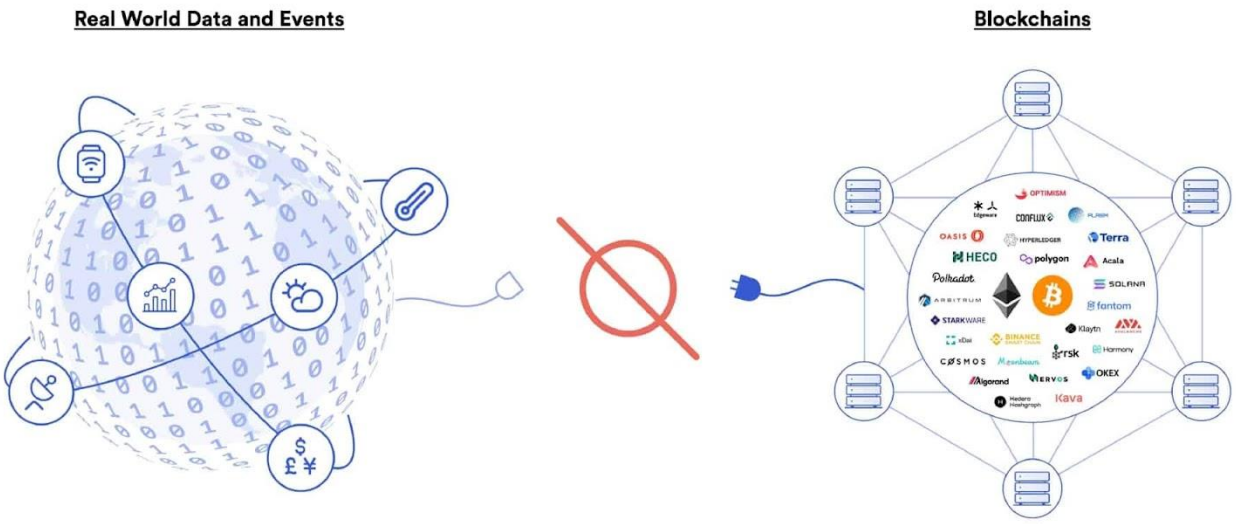


Blockchain oracles connect blockchains to inputs and outputs in the real world

For example, let's assume Alice and Bob want to bet on the outcome of a sports match. Alice bets $20 on team A and Bob bets $20 on team B, with the $40 total held in escrow by a smart contract. When the game ends, how does the smart contract know whether to release the funds to Alice or Bob? The answer is it requires an oracle mechanism to fetch accurate match outcomes offchain and deliver it to the blockchain in a secure and reliable manner.

Solving the Oracle Problem

The blockchain oracle problem outlines a fundamental limitation of smart contracts—they cannot inherently interact with data and systems existing outside their native blockchain environment. Resources external to the blockchain are considered "offchain," while data already stored on the blockchain is considered onchain. By being purposely isolated from external systems, blockchains obtain their most valuable properties like strong consensus on the validity of user transactions, prevention of double-spending attacks, and mitigation of network downtime. Securely interoperating with offchain systems from a blockchain requires an additional piece of infrastructure known as an "oracle" to bridge the two environments.



Blockchains cannot connect to real-world data and events on their own

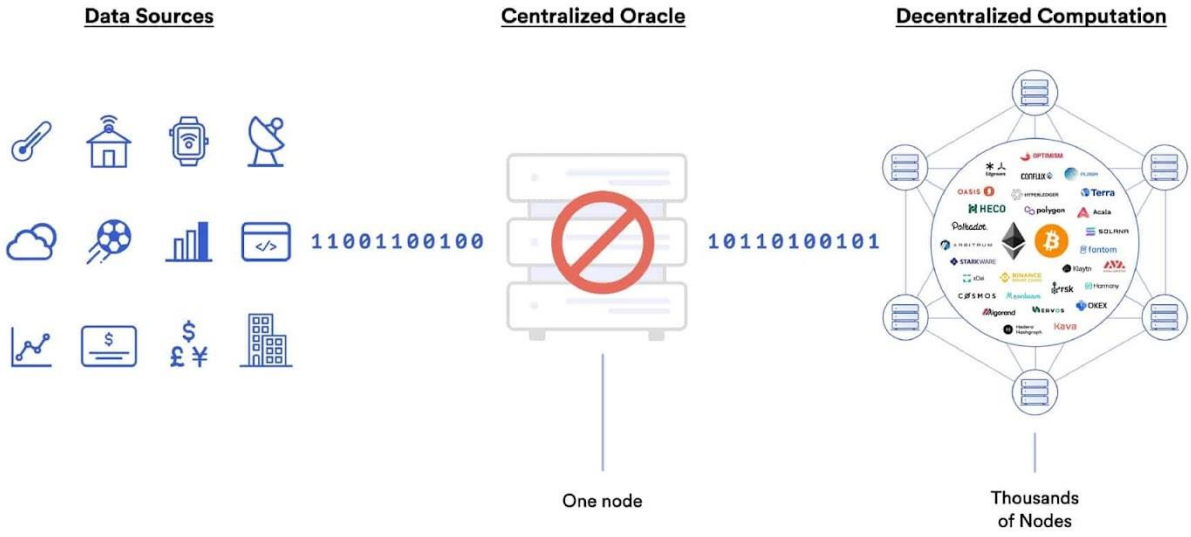
Solving the oracle problem is of the utmost importance because the vast majority of smart contract use cases like DeFi require knowledge of real-world data and events happening offchain. Thus, crypto oracles expand the types of digital agreements that blockchains can support by offering a universal gateway to offchain resources while still upholding the valuable security properties of blockchains. Major industries benefit from combining oracles and smart contracts including asset prices for finance, weather information for insurance, randomness for gaming, IoT sensors for supply chain, ID verification for government, and much more.

Because the data delivered by oracles to blockchains directly determines the outcomes of smart contracts, it is critically important that the oracle mechanism is correct if the agreement is to execute exactly as expected.

Decentralized Oracles

Blockchain oracle mechanisms using a centralized entity to deliver data to a smart contract introduce a single point of failure, defeating the entire purpose of a decentralized blockchain application. If the single oracle goes offline, then the smart contract will not have access to the data required for execution or will execute improperly based on stale data.

Even worse, if the single oracle is corrupted, then the data being delivered onchain may be highly incorrect and lead to smart contracts executing very wrong outcomes. This is commonly referred to as the "garbage in, garbage out" problem where bad inputs lead to bad outputs. Additionally, because blockchain transactions are automated and immutable, a smart contract outcome based on faulty data cannot be reversed, meaning user funds can be permanently lost. Therefore, centralized oracles are a non-starter for smart contract applications.



Centralized oracles are a single point of failure

Truly overcoming the crypto oracle problem necessitates decentralized oracles to prevent data manipulation, inaccuracy, and downtime. A Decentralized Oracle Network,

or DON for short, combines multiple independent oracle node operators and multiple reliable data sources to establish end-to-end decentralization.

DONs enable the creation of hybrid smart contracts, where onchain code and offchain infrastructure are combined to support advanced decentralized applications (dApps) that react to real-world events and interoperate with traditional systems.

Many Chainlink services, such as Chainlink Price Feeds, incorporate three layers of decentralization—at the data source, individual node operator, and oracle network levels—to eliminate any single point of failure. Chainlink Price Feeds already help secure tens of billions of dollars across smart contract ecosystems through this multi-layered decentralization approach, ensuring smart contracts can safely rely on data inputs during their execution.

Chainlink Price Feeds deploy three layers of decentralized aggregation

Types of Blockchain Oracles

Given the extensive range of offchain resources, blockchain oracles come in many shapes and sizes. Not only do hybrid smart contracts need various types of external data and computation, but they require various mechanisms for delivery and different levels of security. Generally, each type of crypto oracle involves some combination of fetching, validating, computing upon, and delivering data to a destination.

Input Oracles

The most widely recognized type of oracle today is known as an "input oracle," which fetches data from the real-world (offchain) and delivers it onto a blockchain network for smart contract consumption. These types of oracles are used to power Chainlink Price Feeds, providing DeFi smart contracts with onchain access to financial market data.

Output Oracles

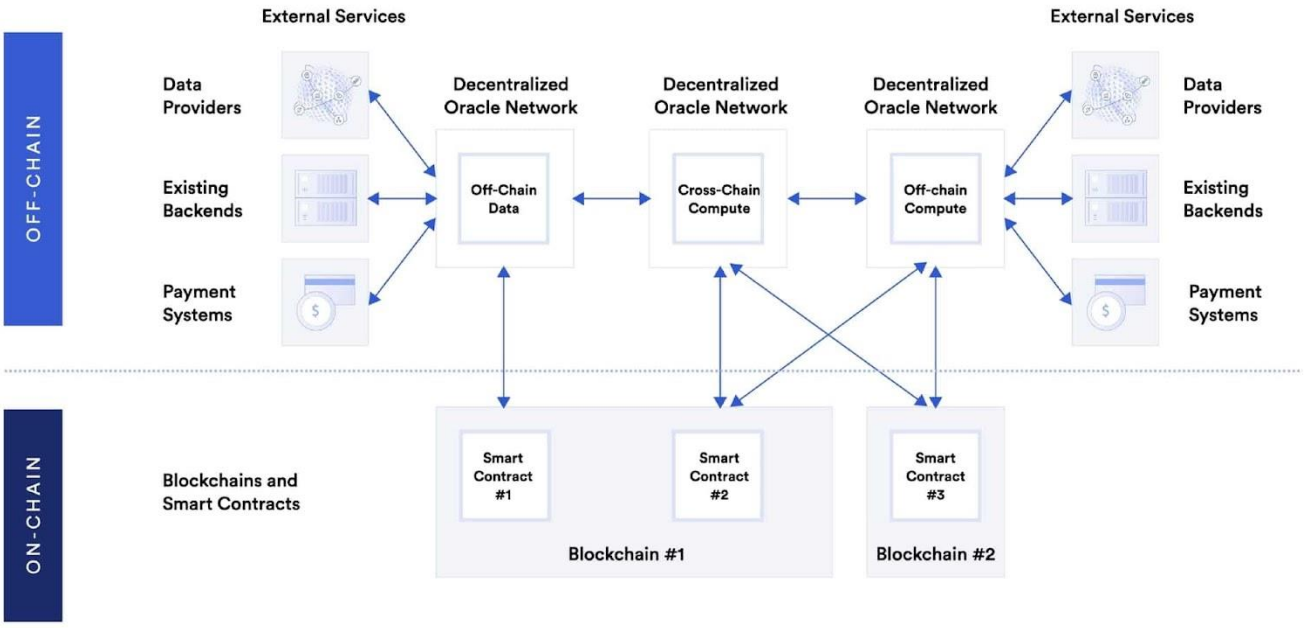
The opposite of input oracles are "output oracles," which allow smart contracts to send commands to offchain systems that trigger them to execute certain actions. This can include informing a banking network to make a payment, telling a storage provider to store the supplied data, or pinging an IoT system to unlock a car door once the onchain rental payment is made.

Cross-Chain Oracles

Another type of oracle are cross-chain oracles that can read and write information between different blockchains. Cross-chain oracles enable interoperability for moving both data and assets between blockchains, such as using data on one blockchain to trigger an action on another or bridging assets cross-chain so they can be used outside the native blockchain they were issued on.

Compute-Enabled Oracles

A new type of oracle becoming more widely used by smart contract applications are "compute-enabled oracles," which use secure offchain computation to provide decentralized services that are impractical to do onchain due to technical, legal, or financial constraints. This can include using Chainlink Automation to trigger the running of smart contracts when predefined events take place, computing zero-knowledge proofs to generate data privacy, or running a verifiable randomness function to provide a tamper-proof and provably fair source of randomness to smart contracts.



Different types of oracles enable the creation of hybrid smart contracts

Oracle Reputation Derived From Onchain Performance History

The broad range of oracle services means reputation is key to choosing between oracle service providers. Reputation in blockchain oracle systems gives users and developers the ability to monitor and filter between oracles based on parameters they deem

important. Oracle reputation is aided by the fact that oracles sign and deliver their data onto an immutable public blockchain ledger, and so their historical performance history can be analyzed and presented to users through interactive dashboards.

Reputation frameworks provide transparency into the accuracy and reliability of each oracle network and individual oracle node operator. Users can then make informed decisions about which oracles they want to service their smart contracts. Oracle service providers can also leverage their offchain business reputation to provide users additional guarantees of their reliability.

Blockchain Oracle Use Cases

Smart contract developers use oracles to build more advanced decentralized applications across a wider range of blockchain use cases. While there are a potentially infinite number of possibilities, below are the use cases with the most current adoption.

Decentralized Finance (DeFi)

A large portion of the decentralized finance (DeFi) ecosystem requires price oracles so smart contracts can access financial data about assets and markets. For example, decentralized money markets use price oracles to determine users' borrowing capacity and check if users' positions are undercollateralized and subject to liquidation. Similarly, synthetic asset platforms use price oracles to peg the value of tokens to real-world assets and automated market makers (AMMs) use price oracles to help concentrate liquidity at the current market price to improve capital efficiency.

Dynamic NFTs and Gaming

Oracles enable non-financial use cases for smart contracts too such as dynamic NFTs—Non-Fungible Tokens that can change in appearance, value, or distribution based on external events like the time of day or the weather. Additionally, compute oracles are used to generate verifiable randomness that projects then use to assign randomized traits to NFTs or to select random lucky winners in high-demand NFT drops. Onchain gaming applications also use verifiable randomness to create more engaging and unpredictable gameplay experiences like the appearance of random loot boxes or randomized matchmaking during a tournament.

Insurance

Insurance smart contracts use input oracles to verify the occurrence of insurable events during claims processing, opening up access to physical sensors, web APIs, satellite imagery, and legal data. Output oracles can also provide insurance smart contracts with a way to make payouts on claims using other blockchains or traditional payment networks.

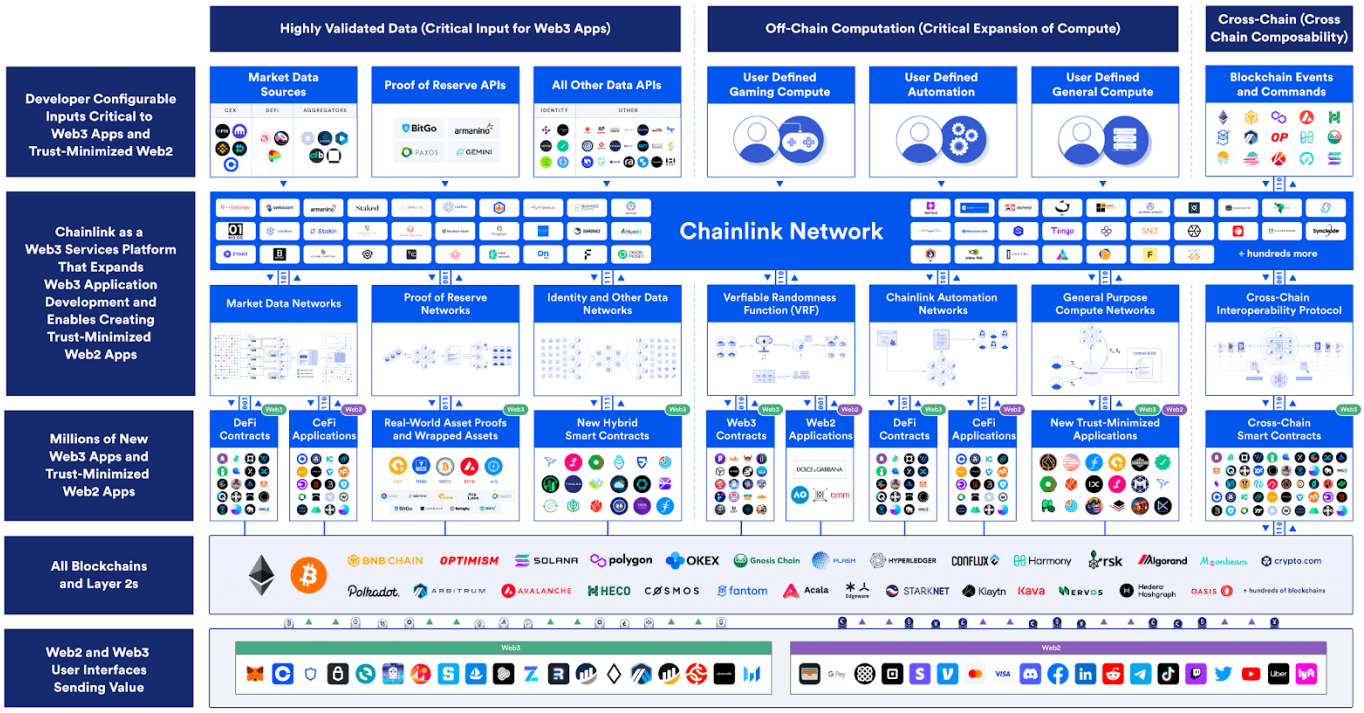
Enterprise

Cross-chain oracles offer enterprises a secure blockchain middleware that allows them to connect their backend systems to any blockchain network. In doing so, enterprise systems can read/write to any blockchain and perform complex logic on how to deploy

assets and data across chains and with counterparties using the same oracle network. The result is institutions being able to quickly join blockchains in high demand by their counterparties and swiftly create support for smart contract services wanted by their users without having to spend time and development resources integrating with each individual blockchain.

Sustainability

Hybrid smart contracts are advancing environmental sustainability by creating better incentives to partake in green practices through advanced verification techniques around the true impact of green initiatives. Oracles are a critical tool to supplying smart contracts with environmental data from sensor readings, satellite imagery, and advanced ML computation, which then allow smart contracts to dispense rewards to people practicing reforestation or engaging in conscious consumption. Oracles are also supporting many new forms of carbon credits to offset the impacts of climate change.



Chainlink's growing collection of decentralized oracle services

Oracles extend the capabilities of blockchain networks by providing access to all the external resources required to harness useful and advanced hybrid smart contract use cases beyond simple tokenization. Similar to how the Internet brought forth a significant change in the way information is exchanged, oracle-powered hybrid smart contracts are redefining the way society exchanges value and enforces contractual agreements.

What Is An NFT? Non-Fungible Tokens Explained

Non-fungible tokens (NFTs) seem to be everywhere these days. From art and music to tacos and toilet paper, these digital assets are selling like 17th-century exotic Dutch tulips—some for millions of dollars.

But are NFTs worth the money—or the hype? Some experts say they're a bubble poised to pop, like the dot-com craze or Beanie Babies. Others believe NFTs are here to stay, and that they will change investing forever.

What Is an NFT?

An NFT is a digital asset that can come in the form of art, music, in-game items, videos, and more. They are bought and sold online, frequently with cryptocurrency, and they are generally encoded with the same underlying software as many cryptos.

Although they've been around since 2014, NFTs are gaining notoriety now because they are becoming an increasingly popular way to buy and sell digital artwork. The market for NFTs was worth a staggering $41 billion in 2021 alone, an amount that is approaching the total value of the entire global fine art market.

NFTs are also generally one of a kind, or at least one of a very limited run, and have unique identifying codes. "Essentially, NFTs create digital scarcity," says Arry Yu, chair of the Washington Technology Industry Association Cascadia Blockchain Council and managing director of Yellow Umbrella Ventures.

This stands in stark contrast to most digital creations, which are almost always infinite in supply. Hypothetically, cutting off the supply should raise the value of a given asset, assuming it's in demand.

But many NFTs, at least in these early days, have been digital creations that already exist in some form elsewhere, like iconic video clips from NBA games or securitized versions of digital art that's already floating around on Instagram.

Famous digital artist Mike Winklemann, better known as "Beeple," crafted a composite of 5,000 daily drawings to create perhaps the most famous NFT of 2021, "EVERYDAYS: The First 5000 Days," which sold at Christie's for a record-breaking $69.3 million.

Anyone can view the individual images—or even the entire collage of images online for free. So why are people willing to spend millions on something they could easily screenshot or download?

Because an NFT allows the buyer to own the original item. Not only that, it contains built-in authentication, which serves as proof of ownership. Collectors value those "digital bragging rights" almost more than the item itself.

How Is an NFT Different from Cryptocurrency?

NFT stands for non-fungible token. It's generally built using the same kind of programming as cryptocurrency, like Bitcoin or Ethereum, but that's where the similarity ends.

Physical money and cryptocurrencies are "fungible," meaning they can be traded or exchanged for one another. They're also equal in value—one dollar is always worth another dollar; one Bitcoin is always equal to another Bitcoin. Crypto's fungibility makes it a trusted means of conducting transactions on the blockchain.

NFTs are different. Each has a digital signature that makes it impossible for NFTs to be exchanged for or equal to one another (hence, non-fungible). One NBA Top Shot clip, for example, is not equal to EVERYDAYS simply because they're both NFTs. (One NBA Top Shot clip isn't even necessarily equal to another NBA Top Shot clip, for that matter.)

How Does an NFT Work?

NFTs exist on a blockchain, which is a distributed public ledger that records transactions. You're probably most familiar with blockchain as the underlying process that makes cryptocurrencies possible.

Specifically, NFTs are typically held on the Ethereum blockchain, although other blockchains support them as well.

An NFT is created, or "minted" from digital objects that represent both tangible and intangible items, including:

- Grafic art
- GIFs
- Videos and sports highlights
- Collectibles
- Virtual avatars and video game skins
- Designer sneakers
- Music

Even tweets count. Twitter co-founder Jack Dorsey sold his first ever tweet as an NFT for more than $2.9 million.

Essentially, NFTs are like physical collector's items, only digital. So instead of getting an actual oil painting to hang on the wall, the buyer gets a digital file instead.

They also get exclusive ownership rights. NFTs can have only one owner at a time, and their use of blockchain technology makes it easy to verify ownership and transfer tokens between owners. The creator can also store specific information in an NFT's metadata. For instance, artists can sign their artwork by including their signature in the file.

What Are NFTs Used For?

Blockchain technology and NFTs afford artists and content creators a unique opportunity to monetize their wares. For example, artists no longer have to rely on galleries or auction houses to sell their art. Instead, the artist can sell it directly

to the consumer as an NFT, which also lets them keep more of the profits. In addition, artists can program in royalties so they'll receive a percentage of sales whenever their art is sold to a new owner. This is an attractive feature as artists generally do not receive future proceeds after their art is first sold.

Art isn't the only way to make money with NFTs. Brands like Charmin and Taco Bell have auctioned off themed NFT art to raise funds for charity. Charmin dubbed its offering "NFTP" (non-fungible toilet paper), and Taco Bell's NFT art sold out in minutes, with the highest bids coming in at 1.5 wrapped ether (WETH)—equal to $3,723.83 at time of writing.

Nyan Cat, a 2011-era GIF of a cat with a pop-tart body, sold for nearly $600,000 in February. And NBA Top Shot generated more than $500 million in sales as of late March. A single LeBron James highlight NFT fetched more than $200,000.

Even celebrities like Snoop Dogg and Lindsay Lohan are jumping on the NFT bandwagon, releasing unique memories, artwork and moments as securitized NFTs.

How to Buy NFTs

If you're keen to start your own NFT collection, you'll need to acquire some key items:

First, you'll need to get a digital wallet that allows you to store NFTs and cryptocurrencies. You'll likely need to purchase some cryptocurrency, like Ether, depending on what currencies your NFT provider accepts. You can buy crypto using a credit card on platforms like Coinbase, Kraken, eToro and even PayPal and Robinhood now. You'll then be able to move it from the exchange to your wallet of choice.

You'll want to keep fees in mind as you research options. Most exchanges charge at least a percentage of your transaction when you buy crypto.

Popular NFT Marketplaces

Once you've got your wallet set up and funded, there's no shortage of NFT sites to shop. Currently, the largest NFT marketplaces are:

• **OpenSea.io**: This peer-to-peer platform bills itself a purveyor of "rare digital items and collectibles." To get started, all you need to do is create an account to browse NFT collections. You can also sort pieces by sales volume to discover new artists.

• **Rarible**: Similar to OpenSea, Rarible is a democratic, open marketplace that allows artists and creators to issue and sell NFTs. RARI tokens issued on the platform enable holders to weigh in on features like fees and community rules.

• **Foundation**: Here, artists must receive "upvotes" or an invitation from fellow creators to post their art. The community's exclusivity and cost of entry—artists must also purchase "gas" to mint NFTs—means it may boast higher-caliber artwork. For instance, Nyan Cat creator Chris Torres sold the NFT on the Foundation platform. It may also mean higher prices — not necessarily a bad thing for artists and collectors seeking to capitalize, assuming the demand for NFTs remains at current levels, or even increases over time.

Although these platforms and others are host to thousands of NFT creators and collectors, be sure you do your research carefully before buying. Some artists have fallen victim to impersonators who have listed and sold their work without their permission.

In addition, the verification processes for creators and NFT listings aren't consistent across platforms — some are more stringent than others. OpenSea and Rarible, for example, do not require owner verification for NFT listings. Buyer protections appear to be sparse at best, so when shopping for NFTs, it may be best to keep the old adage "caveat emptor" (let the buyer beware) in mind.

Should You Buy NFTs?

Just because you can buy NFTs, does that mean you should? It depends, Yu says.

"NFTs are risky because their future is uncertain, and we don't yet have a lot of history to judge their performance," she notes. "Since NFTs are so new, it may be worth investing small amounts to try it out for now."

In other words, investing in NFTs is a largely personal decision. If you have money to spare, it may be worth considering, especially if a piece holds meaning for you.

But keep in mind, an NFT's value is based entirely on what someone else is willing to pay for it. Therefore, demand will drive the price rather than fundamental, technical or economic indicators, which typically influence stock prices and at least generally form the basis for investor demand.

All this means, an NFT may resale for less than you paid for it. Or you may not be able to resell it at all if no one wants it.

NFTs are also subject to capital gains taxes—just like when you sell stocks at a profit. Since they're considered collectibles, however, they may not receive the preferential long-term capital gains rates stocks do and may even be taxed at a higher collectibles tax rate, though the IRS has not yet ruled what NFTs are considered for tax purposes. Bear in mind, the cryptocurrencies used to purchase the NFT may also be taxed if they've increased in value since you bought them, meaning you may want to check in with a tax professional when considering adding NFTs to your portfolio.

That said, approach NFTs just like you would any investment: Do your research, understand the risks—including that you might lose all of your investing dollars—and if you decide to take the plunge, proceed with a healthy dose of caution.

What Are DAOs and Why You Should Pay Attention

Jun 1, 2021,08:00am EDT

Updated May 16, 2022, 10:03am EDT

Can you imagine a way of organizing with other people around the world, without knowing each other and establishing your own rules, and making your own decisions autonomously all encoded on a Blockchain? Well, DAOs are making this real.

Wikipedia defines DAO (Decentralized Autonomous Organization) as an organization represented by rules encoded as a transparent computer program, controlled by the organization members, and not influenced by a central government. As the rules are embedded into the code, no managers are needed, thus removing any bureaucracy or hierarchy hurdles.

Some of today's internet users and the next generations are looking forward to starting social organizations, searching for an answer to: "How can we exchange values in a trusted environment?"Blockchain enables automated trusted transactions and value exchanges, but even so, internet users around the world want to organize themselves in a "Safe and effective way to work with like-minded folks, around the globe", according to Ethereum

Bitcoin is generally considered to be the first fully functional DAO, as it has programmed rules, functions autonomously, and is coordinated through a consensual protocol. Of course, not every DAO has been as successful as Bitcoin. In May 2016, German startup slock.it launched the creatively named "The DAO" in support of their decentralized version of Airbnb. At the time it was a great success with a crowdfunding campaign that raised over $150 million worth of Ethereum.

Unfortunately, the code they used in the DAO had certain issues. So inevitably in June 2016 hackers managed to siphon off $50 million worth of Ethereum from the DAO before it was stopped. Even though the fault was in the slock.it code and not in the underlying technology, the hack did undermine some people's trust in both the Ethereum coin and DAOs in general.

But today, due to the explosion of Decentralized Finance (DeFi) during 2020, has led to a rise in renewed interest in DAOs. Now that you have a better idea of what DAOs are, it is important to understand more about their background and characteristics to appreciate the whole picture of what is turning traditional forms of organizing upside down.

What Makes DAOs Different?

A DAO's financial transactions and rules are recorded on a blockchain. This eliminates the need to involve a third party in a financial transaction, simplifying those transactions through smart contracts. The firmness of a DAO is a smart contract. The smart contract represents the rules of the organization and holds the Organization's storage. No one can edit the rules without people noticing, because DAOs are transparent and public. Up to today we are used to companies backed by

legal status, a DAO may perfectly function without it as it can be structured as a general partnership.

In comparison to traditional companies, DAOs have a democratized organization. All the members of a DAO need to vote for any changes to be implemented, instead of implemented changes by a sole party (depending on the company's structure). The funding of DAOs is mainly based on crowdfunding that issues tokens. The governance of DAOs is based on community, while traditional companies' governance is mostly based on executives, Board of Directors, activist investors. etc. DAOs' operations are fully transparent and global, meanwhile, traditional companies' operations are private, only the organization know what is happening, and they are not always global.

Fully Functional DAOs

DAOs need the following elements for being fully functional: A set of rules to which will operate, a funding like tokens that the organization can spend to reward certain activities to their members, and also to provide voting rights for establishing the operation rules. Also, and most important, is a well and secure structure that allows every investor to configure the organization.

One potential problem with the voting system is that even if a security hole was spotted in its initial code, it can't be corrected until the majority votes on it. While the voting process takes place, hackers can make use of a bug in the hole of the code.

How Are DAOs Being Used Today?

So far DAOs are being used for many purposes such as investment, charity, fundraising, borrowing, or buying NFTs, all without intermediaries. So you can have a better idea, for example, a DAO can accept donations from anyone around the world and the members can decide how to spend donations.

Can you imagine being a co-owner of an Artist's song by just using cryptocurrency on an internet-based organization? In May 2021, Jenny DAO acquired its first NFT, an original song of Steve Aoki and 3LAU. This DAO is a metaverse organization that provides fractional ownership of NFTs. Its members will be able to oversee the purchase of the NFTs and Unicly protocol's smart contracts control the vault where these NFTs will be added.

The Metaverse Is Changing Business As We Know It

DAOs envision a collective organization owned and managed by its members with all of them having a voice. Many analysts and industry insiders affirm that this type of organization is coming to prominence, even potentially replacing some traditional companies.

Businesses and brands need to stay abreast of current trends that could impact how they engage with consumers and how consumers interact with them. While DAOs are not ubiquitous yet, they do seem to be picking up steam with many creators.

Decentralized Applications (dApps): Definition, Uses, Pros and Cons

What Are Decentralized Applications (dApps)?

Decentralized applications, or dApps, are software programs that run on a blockchain or peer-to-peer (P2P) network of computers instead of on a single computer. Rather than operating under the control of a single authority, dApps are spread across the network to be collectively controlled by its users. They are often built on the Ethereum platform and have been developed for various purposes, including wallets, exchanges, gaming, personal finance, and social media.

Understanding Decentralized Applications (dApps)

A web app such as Uber or X (formerly Twitter) runs on a computer system that is owned and operated by a company with authority over the app and its workings. No matter how many users there are, the backend is controlled by the company.

DApps operate a bit differently. They run on a P2P or a blockchain network. For example, BitTorrent, Tor, and Popcorn Time are applications that run on computers that are part of a P2P network, which allows multiple participants to consume, feed, or seed content.

DApps are similar but run on a blockchain network in a public, open-source, decentralized environment. They are free from control and interference by any single authority. For example, a developer can create an X-like dApp and put it on a blockchain where any user can publish messages. Once posted, no one except the message originator can delete the messages.

Difference Between a Centralized and Decentralized App

A centralized app has a single owner. The application software for a centralized app resides on one or more servers controlled by the owner. Users interact with the app by downloading a copy of it and then sending and receiving data back and forth from the company's server.

A decentralized app operates on a blockchain or peer-to-peer network of computers. Users engage in transactions directly with one another rather than relying on a central authority to facilitate them. The dApp might be free, or the user might need to pay the developer in cryptocurrency to download and use the program's source code. The

source code nearly always uses smart contracts, which complete transactions between people. Smart contracts remove the need to trust that the other party will execute their part of a transaction. The apps also rely on blockchain protocols that hide personal information.

Importance of dApps

There are several dApp features that can dramatically change the facilitation of information or resources.

Cost and Efficiency

Because dApps operate on decentralized networks, there is no need for an intermediary. This can lead to reduced costs, increased efficiency, and greater accessibility. For example, instead of having to rely on a bank, imagine having nearly 100% control of every aspect of your finances. This can have major implications for many industries, especially the financial sector.

Security

Because dApps leverage blockchain technology, these solutions can also help improve security in many business and personal processes. Blockchains make data immutable by leveraging cryptographic techniques and distributed automated consensus. Because the ledger is shared and compared across all users, data cannot be altered.

Accessibility

DApps are accessible to anyone with an internet connection. It doesn't matter where you live—all you need is internet access. This global accessibility democratizes access to many different types of services, digital assets, and information.

Transparency

Blockchain-based dApps maintain transparent records of transactions, meaning users can verify the integrity of data without relying on centralized authorities. This transparency is critical for distributed and anonymous networks because users need to know the system is trustworthy.

DApp Uses

DApps have been developed to decentralize a range of functions and applications and eliminate intermediaries. Examples include self-executing financial contracts, multi-user games, and social media platforms.

DApps have also been developed to enable secure, blockchain-based voting and governance. They can even be integrated into web browsers to function as plugins that help serve ads, track user behavior, or solicit crypto donations.

Some examples of practical uses for dApps include:

- **Financial services**: Facilitating peer-to-peer financial transactions, such as currency exchanges or asset transfers.

- **Supply chain management**: Tracking the movement of goods through a supply chain, ensuring transparency and accountability.
- **Identity verification**: Securely storing and verifying identity information, such as for voter rolls or passport applications.
- **Real estate**: Facilitating real estate transactions directly between buyer and seller, tracking property ownership and related documentation, such as deeds.
- **Healthcare**: Storing and tracking healthcare records and facilitating communications between healthcare professionals.
- **Education**: Creating decentralized learning platforms that allow students and teachers to interact and collaborate directly without the need for intermediaries.
- **Social media**: Creating decentralized social media platforms that allow users to interact and share content without being censored by a centralized authority.
- **Predictive markets**: Creating decentralized platforms for predictive markets, allowing users to make bets on any event.

Scams Involving dApps

Scams have been perpetrated through dApps. Ponzi schemes, in which early investors are paid using the investments of more recent investors to create the appearance of big profits, have been known to occur on dApps.

Fake initial coin offerings (ICOs) have been used to raise funds for developing a new cryptocurrency or dApp that the fundraisers have no intention of creating.

Phishing attacks, which use fake websites or emails to trick people into revealing sensitive information, have been seen on dApps. In addition, some dApps have been used to distribute malware or viruses, which can compromise users' devices and steal sensitive information.

Users should be cautious and do their due diligence when interacting with dApps, as the decentralized nature of these applications can make it difficult to track or hold perpetrators accountable.

Advantages and Disadvantages of dApps

Advantages

Many of the advantages of dApps center around their ability to safeguard user privacy. DApps use smart contracts to complete transactions between two anonymous parties.

Free speech proponents point out that dApps can be developed as alternative social media platforms. A decentralized social media platform is resistant to censorship because no single participant on the blockchain can delete or block messages.

Ethereum is a flexible platform for creating new dApps, providing the infrastructure needed for developers to focus their efforts on finding innovative uses for digital

applications. This could enable the rapid deployment of dApps in several industries, including banking and finance, gaming, social media, and online shopping.

Disadvantages

DApps are still in the early stages, so they are experimental and prone to certain problems and unknowns. Questions arise about whether the applications will be able to scale effectively. Also, there are concerns that too many applications requiring computational resources will overload a network, causing congestion.

The ability to develop a user-friendly interface is another concern. Most apps developed by traditional centralized institutions have an ease-of-use expectation that encourages users to use and interact with the app. Getting people to transition to dApps will require developers to create an end-user experience and level of performance that rivals popular and established programs.

Because they are decentralized, dApps are not subject to the oversight and auditing most centralized applications are exposed to. If the application's programming is rushed, unaudited, or sloppy, hackers will find it easy to break into it.

Once deployed, a dApp is likely to need ongoing changes to make enhancements or correct bugs or security risks. According to Ethereum, it can be challenging for developers to update dApps because the data and code published to the blockchain are hard to modify.5

Ethereum. "Introduction to Dapps."

Pros

- Promotes user privacy
- Resists censorship
- Flexible platform enables dApp development

Cons

- Experimental, may not be able to scale
- Challenges in developing a user-friendly interface
- Difficult to make needed code modifications
- Security issues if programming is sloppy

Regulatory Considerations for dApps

One of the primary challenges regulators face with dApps is their decentralized nature. Traditional regulatory considerations are usually based on a specific location; since dApps are not centralized, it's tougher to regulate activity based on where transactions occur.

The Emerging Centralization of dApps

Consider the General Data Protection Regulation (GDPR) and its implementation within the European Union. DApp providers that serve the EU audience must comply with GDPR requirements, regardless of their home jurisdiction.

In December 2023, a European subnet of the Internet Computer Protocol (ICP, a blockchain DAO) was launched that provides an infrastructure and set of tools developers can use to create compliant dApps.6 If using the ICP becomes the standard way of ensuring compliance, the apps lose their decentralized standing because the ICP is centralized—nodes must be voted in by the DAO and can only be located in the EU.7

Some dApps issue tokens or conduct token sales to raise money. This may raise regulatory concerns as authorities work to protect investors—it is viewed by regulators as an unregistered securities issuance. In a similar manner, dApps involved in financial services, such as decentralized exchanges (DEXs) or lending platforms, must adhere to anti-money laundering or know-your-client regulations to prevent money laundering and terrorist financing.

Consumer Protection

There is also a consumer protection element even if the user is not exchanging money or goods. This includes personal data, privacy, and security protection. Agreeing to the transactions via signature puts users at risk; platforms such as MetaMask warn users to be aware that they could lose funds if they're unaware of what they agree to when using dApps.8

Example of dApps

One popular example of a dApp is CryptoKitties.9 CryptoKitties is a blockchain-based virtual game that allows players to adopt, raise, and trade virtual cats. The game is one of the world's first forms of interactive blockchain dApps.9

Each CryptoKitty is unique, owned by the user, and validated through the blockchain. Like other types of tradeable assets, its value can appreciate or depreciate based on the market. CryptoKitties are considered "crypto collectibles" because each digital pet is one-of-a-kind and verified on a blockchain.

Another example is Uniswap, a decentralized exchange protocol built on Ethereum.10 Uniswap enables users to trade directly with each other without needing an intermediary, like a bank or broker. This dApp uses automated smart contracts to create liquidity pools that facilitate trades. Users can trade their tokens directly from their wallets, providing a seamless and secure trading experience. Again, the existence of Uniswap is made possible by the decentralized nature of the application.

What Is Meant By Decentralized Application?

Decentralized applications are applications that are generally open source and use or facilitate blockchain and cryptocurrency transactions.

What Is the Most Popular Decentralized Application?

Cryptocurrency wallets like MetaMask are the most popular dApps, followed by exchanges like Uniswap and openSea. Gambling dApps like MetaWin are also very popular.

Is Bitcoin a Decentralized Application?

Bitcoin is decentralized, but it is not an application. It is a blockchain network with a cryptocurrency used as a payment system and speculative investment.

The Bottom Line

Decentralized applications (dApps) are digital applications or programs that run on a decentralized network rather than a single computer or server. They are built on blockchain technology and use cryptocurrency as a means of exchange.

DApps are designed to be open-source, transparent, and resistant to censorship. They allow users to interact directly with the application without intermediaries. DApps have the potential to disrupt traditional industries by allowing for peer-to-peer interactions and transactions without a central authority.

EVM vs Non-EVM Compatible Chains

Introduction

The Ethereum Virtual Machine (EVM) is the runtime environment for smart contracts in Ethereum. It is completely isolated from the main network, which makes the smart contracts safer and more secure. However, not all blockchain networks are EVM-compatible. This article will explore the differences between EVM and non-EVM compatible chains, and delve into the ecosystems that have developed around them.

Ethereum Virtual Machine (EVM)

The EVM is a powerful, Turing complete software that enables developers to run myriad applications on Ethereum. It serves as the backbone of Ethereum, allowing users to write smart contracts in high-level programming languages such as Solidity and Vyper. These contracts are then compiled into bytecode, which the EVM can read and execute.

Ecosystem of EVM-Compatible Chains

EVM-compatible chains, such as Ethereum's rollups (e.g. Arbitrum, Optimism, zkSync, Base), Binance Smart Chain (BSC) and Polygon, benefit from this compatibility in several ways. Firstly, developers can port their applications from Ethereum to these chains with minimal changes. Secondly, these chains can leverage Ethereum's thriving ecosystem of wallets, developer tools, and decentralized applications (dApps).

The ecosystem of EVM-compatible chains is vast and diverse. It includes a wide range of dApps, from decentralized finance (DeFi) platforms, GameFi applications, non-fungible token (NFT) marketplaces to tools. These dApps benefit from the interoperability offered by EVM compatibility, allowing users to seamlessly interact with them across different dApps and chains. Furthermore, the ecosystem also includes a variety of developer tools, which facilitate the development and deployment of dApps on these chains.

Non-EVM Compatible Chains

Non-EVM compatible chains, on the other hand, use different virtual machines and smart contract languages. Examples include the Solana Virtual Machine (SVM) used by Solana, the stack-based virtual machine used by Bitcoin, and the KEVM and IELE virtual machines used by Cardano.

Ecosystem of Non-EVM Compatible Chains

These chains offer unique advantages. For instance, Solana's high throughput and scalability enable the network to handle massive transaction volume. Bitcoin's simplicity makes it highly secure and reliable for transferring value. Cardano's use of formal verification methods offers high assurance of smart contract correctness.

The ecosystems of non-EVM chains are also rich and varied. Solana's ecosystem, for example, includes a wide range of DeFi applications and NFT market place. Cardano's

ecosystem, on the other hand, includes a variety of dApps, stake pools, and NFT market place.

However, these chains also face challenges. The lack of EVM compatibility means that developers cannot easily port their Ethereum applications. They must rewrite their smart contracts in a new language, which can be time-consuming and error-prone. Furthermore, these chains cannot directly leverage Ethereum's ecosystem of developer tools and dApps.

Bridging EVM and Non-EVM Chains

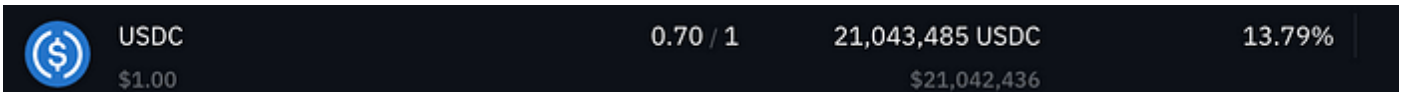
Comparison of TVL on different chains. Source: defillama.com, 19 Feb 2024

Why is it crucial to leverage the developer tools and interoperate with dApps on Ethereum's ecosystem? The above image illustrates the TVL across various chains, clearly showing Ethereum's market dominance. Given Ethereum's fertile ground, it's a natural progression for developers and users to engage with its ecosystem, leading to an enhanced experience and a broader selection of applications.

The need for bridging between EVM and non-EVM chains therefore arises.

Bridging these chains can enable interoperability, allowing dApps to function seamlessly across different chains. This can enhance the user experience, as users can interact with their favorite dApps regardless of the underlying blockchain.

Borrowing rate of USDC at AAVE on Ethereum, 20 Feb 2024



Supply rate of USDC at Solend on Solana, 20 Feb 2024

For instance, there could be interest rate arbitrage across different dApps on various chains. The above images demonstrates an arbitrage opportunity, where an user can

borrow USDC from AAVE on Ethereum at 9.34% and supply to Solend on Solana at 13.79%.

Conclusion

In conclusion, both EVM and non-EVM compatible chains have their strengths and weaknesses. EVM-compatible chains offer high interoperability with Ethereum's thriving ecosystem, making them attractive for developers. Non-EVM chains can offer unique features and advantages, making them appealing for specific use cases. As the blockchain space continues to evolve, there is a rising need to bridge assets across these two ecosystems, we expect more bridges and interoperability solutions that bring these two worlds closer together.

One bridging option is MES Protocol, which provides instant and low-cost asset bridging across EVM and non-EVM compatible chains. Currently it supports Ethereum, Arbitrum, Optimism, zkSync, Base; it plans to extend its support to Solana, Bitcoin and Tron very soon.