

A decorative graphic of a branch with several elongated, pointed leaves, rendered in a light blue line-art style, positioned on the left side of the slide.

Web 3.0

Vedang R. Vatsa FRSA
vedangvats.com



Back in Black

(7th studio album by Australian rock band AC/DC)

- Despite its current popularity, science fiction novelist Neal Stephenson coined the term metaverse thirty years ago in 1992. In his book Snow Crash, the metaverse is described as a 3D virtual environment in which individuals interact with one another and AI-generated characters by walking around as avatars.
- After 30 years, the term has evolved to signify different things in different situations. The metaverse, to put it simply, is a virtual environment where individuals may interact, work, shop, play, etc. Virtual Reality, Augmented Reality, and Digital Reality are the three categories we can use to classify it.



Static Pages
 Frames and Tables
 Few Content Creators
 Banner Ads
 Mostly read-only
 Britannica Online
 HTML

Web 1.0

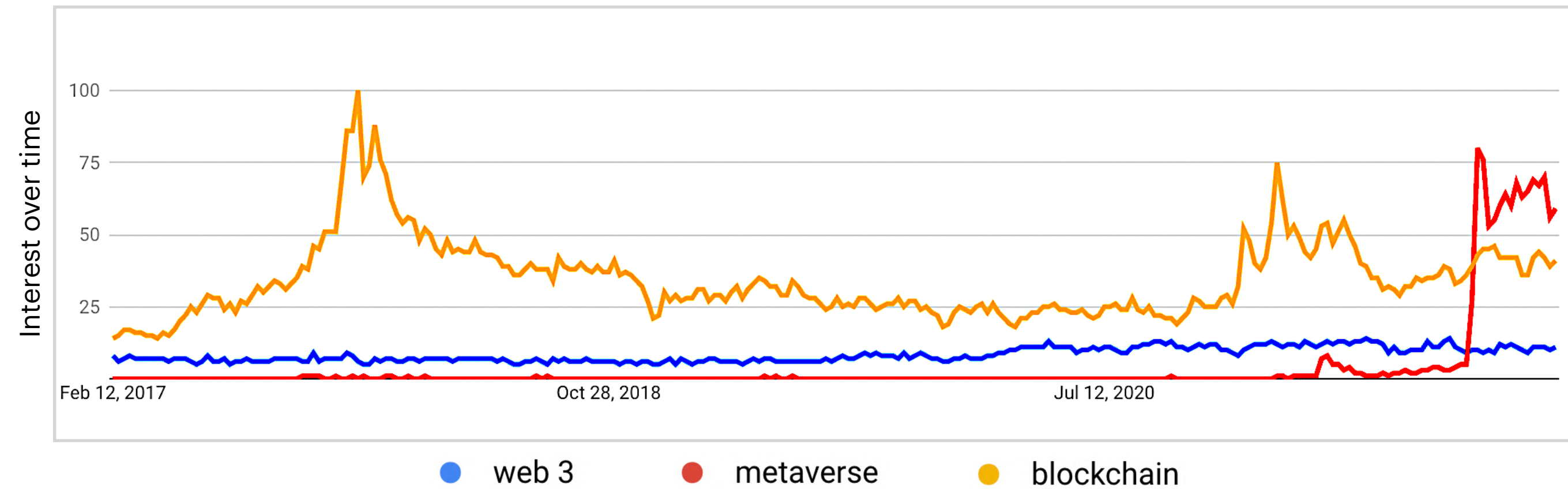
Read and Write
 Web apps
 Interactive Ads
 Wikipedia
 XML/ RSS
 Mobile
 Sharing Economy

Web 2.0

Semantic Web
 Blockchain
 Artificial Intelligence
 Creator Economy
 Decentralisation
 AR & Metaverse
 Privacy and Anonymity
 Custom/ Behavioral Ads

Web 3.0

Google search trends



Top Charts

| | Free Apps | Paid Apps |
|---|--|-----------|
| 1 | Oculus Entertainment | |
| 2 | TikTok Videos, Music & Live Streams | OPEN |
| 3 | YouTube: Watch, Listen, Stream Videos, Music and Live St... | OPEN |
| 4 | Snapchat Share the moment | OPEN |
| 5 | Instagram Photo & Video | OPEN |

The Oculus VR app topped the App Store on Christmas, hinting that Oculus might have been one of the most popular technology gifts.

Internet & Metaverse

| 2D | 3D |
|----------------------------|------------------------|
| Centralised | Decentralised |
| Fiat | Crypto/ DeFi |
| Static/ Dynamic | Real-time |
| Email-Ids and Usernames | Wallets and Avatars |

Virtual Reality

VR is a kind of immersive virtual universe that allows you to touch, feel, and move around in a digital environment using headsets and haptic technologies

- In October 2021, Facebook rebranded itself as "Meta" in order to develop its own version of the metaverse, spending \$10 billion to do so. "Horizon Worlds," their major virtual reality game, is a collaborative world-building playground that can be accessed with Meta's Oculus headset; it went live in December 2021 after an invite-only testing period.
- Oculus was the #1 Free App in Apple's App Store on Christmas Day, demonstrating the return of interest in experiencing the metaverse in the form of virtual reality.



Augmented Reality

AR is an interactive experience in which computer-generated objects and surroundings are superimposed over the real world.



- Pokemon GO (developed by Niantic) grabbed everyone's attention in 2016, with 232 million users at its height and an augmented reality experience at its heart. Players may wander around the real/physical world to catch pokemon that appeared in the app on their phones.
- Snapchat has long been known for its AR-first strategy and filters. Only 0.08% of their customers purchased their AR device, Spectacles, in 2017, and they're no longer for sale; only AR artists on their platform have access to them. Their Lens Studio (AR division), on the other hand, has 200,000 artists who have built 2 million lenses for their 200 million DAUs. Every day, users of the Snapchat app utilise lenses to augment their view of the world.

Digital Reality

This is the metaverse's most open interpretation. Avatars, skins, economies, and social networks in traditional games may all be considered metaverses.



- "If you consider Halo as a game, it is a metaverse," says Microsoft CEO Satya Nadella. "Minecraft is a metaverse".
- In addition to newer games-turned-metaverses like Roblox or Fortnite, which now offer virtual concerts, there are blockchain-based games and worlds (such as Axie Infinity and Sandbox) that are allowing the construction of new worlds that help integrate the digital and real worlds.
- To put it another way, completely digital worlds with digital representation.

A stylized graphic of a branch with several elongated, pointed leaves, rendered in a light teal color. The leaves are arranged in a fan-like pattern, extending from the left side of the frame towards the center.

Cryptocurrency

Crypto: for a 5th grader

Imagine a situation when Rajesh, your best friend, has gone on a vacation abroad and calls you after a week saying that he has run out of cash and requires you to send him some money.

You contact your bank, either by calling your relationship or account manager, or by going there physically or via any online medium, like a website or mobile app. You ask the bank representative to transfer Rs. 50,000 to Rajesh's account. The representative checks the register to see if you have enough balance to make the transfer. After a satisfactory check, he goes on to make an entry in the register stating the details of the required transaction. In a more developed city, this task can be done via computers as well.

"Rajesh, I've transferred you the asked money. Get me a gift when you return back," you said to your friend.

Let's quickly review what happened: You and Rajesh trusted the bank to manage your money. There was no real movement of physical currency, just an entry in a register that neither you nor Rajesh owns or controls.

In other words, you both trusted a third party to enable trust among yourself. The trust among you is dependent on a third party – a middleman.

So, just in case, if we come across a joker in our Gotham city, whose intention is to inject chaos into the society, there are only a few of these organizations/ middlemen to go corrupt (intentionally or not). Also,

What if the register gets burned or lost?

What if the bank representative makes a mistake and enters 10,000 instead of 50,000?

Aren't we relying too much on these middlemen to enable functionality where they need not be involved?

Let's try to simplify the issue here by answering some fundamental questions. Does the transfer of money simply require an entry in a register? What if we could make the entry ourselves instead of asking someone else to do it?

Blockchain aims to answer it by allowing us to maintain the register ourselves instead of being dependent on any third party.

Crypto: for a 5th grader

“

It might make sense just to get some Bitcoin in case it catches on. If enough people think the same way, that becomes a self-fulfilling prophecy.

”

—Satoshi Nakamoto in 2009

So, the main requirement of this method is to have enough people who'd not like to be dependent on these third-party actors.

Let us consider that we found 6 people who'd like to give up their dependency on banks or other such middlemen. Upon a mutual agreement, they get the details of everyone's accounts but without knowing the respective identities of others.

Everyone gets an empty register with spaces where they can add details.

Person2 wants to send Rs. 1000 to Person5. He shouts that he wishes to do so and asks everyone to make an entry for it in their register. Everyone checks whether Person2 has enough money in his/ her account to enable the transaction. After that, they all make a note of this transaction. That's it. That was the end of the first transaction.

Then, after rounds of such shouting and transferring of money, everyone's register starts running out of empty spaces to enter any new transaction. This is the time when everyone secures their current registers and gets a new one. The process of securing can be done via sealing it with a 'unique key.' Sealing is basically an act of securing it so that no one can EVER alter any entry once it is kept in a safe location. For everyone to keep trusting the content of all the registers, they need to trust the sealing process.

Jargon: Mining is the process that is equivalent to sealing in our example.

Currently, we trust a third party (like a bank) to keep the contents of the register safe. However, in a proposed decentralized arrangement, sealing is the crux of trust.

Let us go deeper into the process of sealing.

Consider a machine that gets input from one side and produces an output from the other side. Let us call it a 'Hash function' machine. The method of producing a random output from an input is unknown to anyone – which is the special thing about this machine. Suppose the machine gets an input – 537, it will produce a unique output, which, let us say is – khsfdj. The process is irreversible, which means that you can never figure out the input from the output.

If we start with a trial and error method and feed the input with random numbers, we'll eventually get the output, but the process is going to be very exhaustive. If done on a computer, it will take a lot of computation power to figure out this number. Let us call these efforts – proof of work, as it is proof that work has been done to evaluate the output. After figuring out this special sealing number, we can be sure that the participants have put in effort and ensured that the content is genuine.

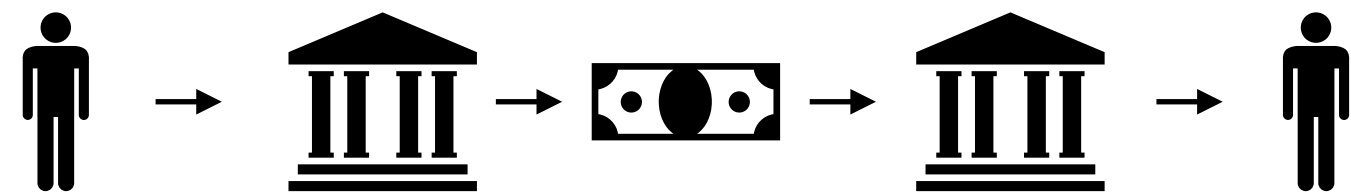
So now we have a mechanism to seal our data of transactions and the actors are also involved in the protection of the contents.

Why put effort into figuring out the sealing number when others can find it eventually? There are rewards associated with it, generally some tokens or coins.

A stylized graphic of a branch with several elongated, pointed leaves, rendered in a light teal color. The branch starts from the bottom left and extends towards the center of the frame.

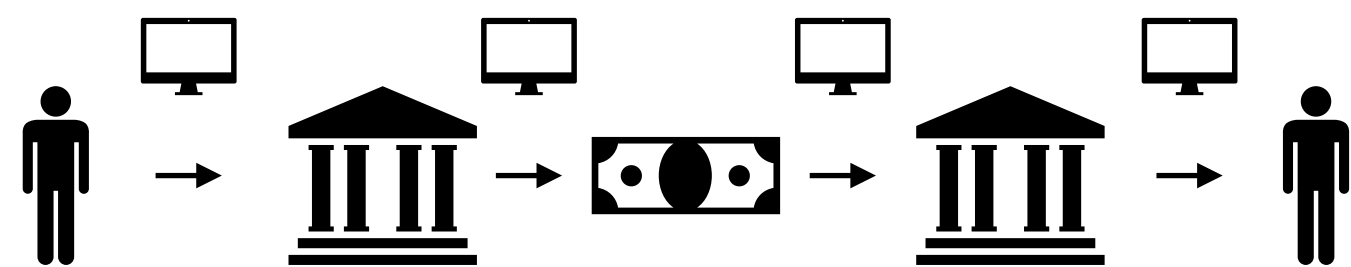
Decentralised Finance

Finance 1.0 v/s Finance 2.0 v/s Finance 3.0



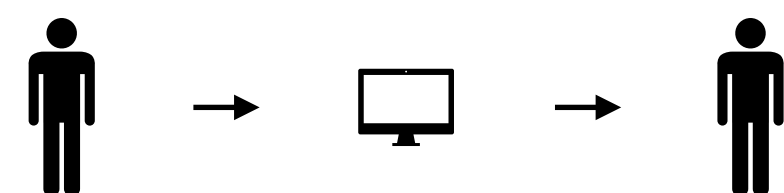
Finance 1.0

- This is the traditional financial system, which began with the establishment of banks and fiat money. We enter the finance 1.0 era, when people began putting their money in banks because they believed banks were more secure than their homes. People began to earn a return on their investment (ROI) by putting their money in the bank, believing that this was the ultimate financial system that we could have.
- Slow transactions, long queues, high transaction fees, time-consuming, the possibility of error (as things were controlled by humans), problems with borderless transactions, robbery, scams, and other issues with finance 1.0 became apparent over time.
- There was no technology in finance 1.0, and all paperwork was handled by humans. The records were kept in register books, which had the risk of being lost or damaged.



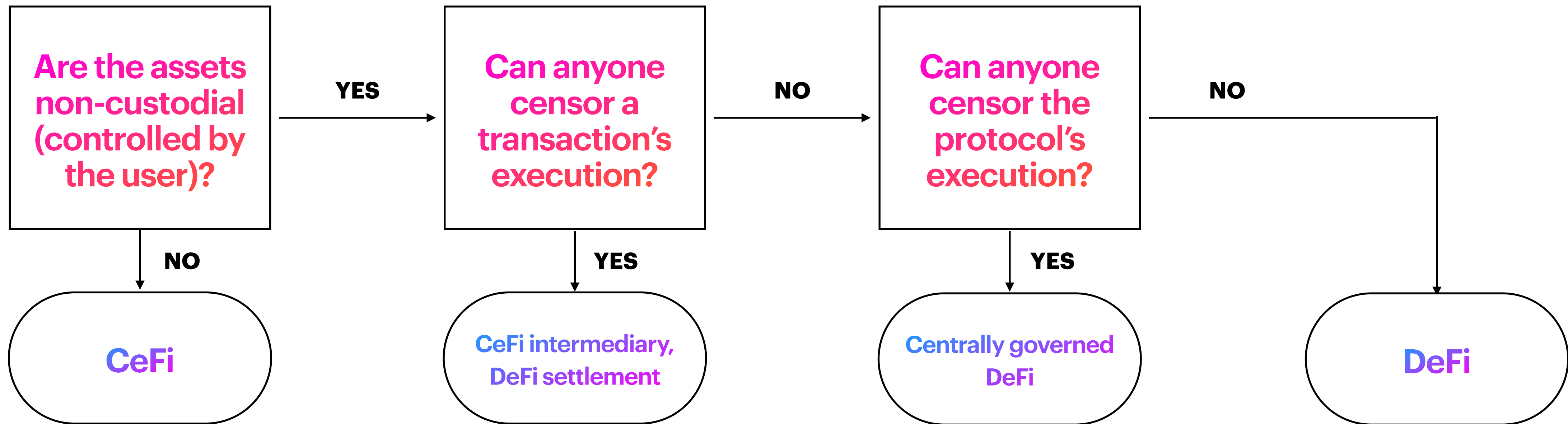
Finance 2.0

- After technology meets finance 1.0, finance 2.0 emerges. Now that everyone has a mobile phone and access to the internet, they can manage all of their financial activities such as money transactions, balance inquiries, complaint registration, money requests, account opening, and so on.
- Many types of third-party payment network processors or payment gateways, such as PayPal, Visa, MasterCard, and others, have been introduced in the era of finance 2.0 to make sending or receiving a payment easier, more convenient, and possible from home.
- The financial system is still not open to the public or under their control. It still has a lot of flaws, such as a centralised system that stores all of the user's data on a centralised server, which often leads to data leakage. Users must pay money in the name of different transaction/processing fees/charges, and users have no control over the money in the bank. The bank has the ability to freeze or invest user funds at any moment in order to generate a profit.



Finance 3.0

- Finance 3.0 is an open financial system that allows customers more power and minimises or eliminates the intermediary, fees, charges, and penalties, among other things. Finance 3.0 is a permissionless system that is not bound by geographical boundaries or social groups.
- To power finance 3.0, we can embrace blockchain technology, which can provide a finance 3.0 system with scalability, transparency, security, and other benefits.



It was in ancient Mesopotamia, more than a thousand years ago, when the concept of centralising financial management was first conceived. A broad variety of items and assets have been used as money since then, including livestock, land, and cowrie shells (a kind of seashell), precious metals (such as gold), and, more recently, fiat currencies. Every effort to build a currency and finance system based on a central authority, such as a government or military, with a military force at its command, has relied on this central authority. Even if a currency's inherent worth is unknown, it may still be valued using an imputed or assumed value, which is an assumed value attributed to a currency, which may be zero.

Rather than requiring customers to put their faith in a third party, decentralised finance relies on financial apps running on top of a distributed blockchain. The main advantage of utilising DeFi is that customers may put their faith in a protocol instead of an organization. Examples are Uniswap, MakerDAO, and Compound. CeFi has a larger level of industry support than DeFi, but Blockchain specialists and technocrats feel that the tables could turn very soon in the future. The introduction of Ethereum allowed businesses to design and deploy projects that established the ecosystem of DeFi, paving the way for the financial sector to maximise the potential of DeFi.

DeFi's advantages over conventional centralised finance include:

- 1. Transparency:** DeFi allows users to look into the specific rules that govern the operation of financial assets and products. Private agreements, back-deals, and centralization are all major barriers to transparency in CeFi, and DeFi seeks to eliminate them.
- 2. Control:** In order to maintain ownership over its users' assets, DeFi ensures that no one may censor, relocate, or destroy the users' assets without the users' permission.
- 3. Accessibility:** While the blockchain and its distributed network of miners effectively administer any DeFi application, anybody with a computer and an internet connection can create and deploy DeFi products.



DAO

Smart Contract

Smart contracts are the programs recorded on a blockchain that execute when certain criteria are fulfilled. They are usually used to automate the execution of an agreement so that all parties can be assured of the result without the participation of any intermediary. Applications include Dispute resolution, Supply chain, and Trade finance.

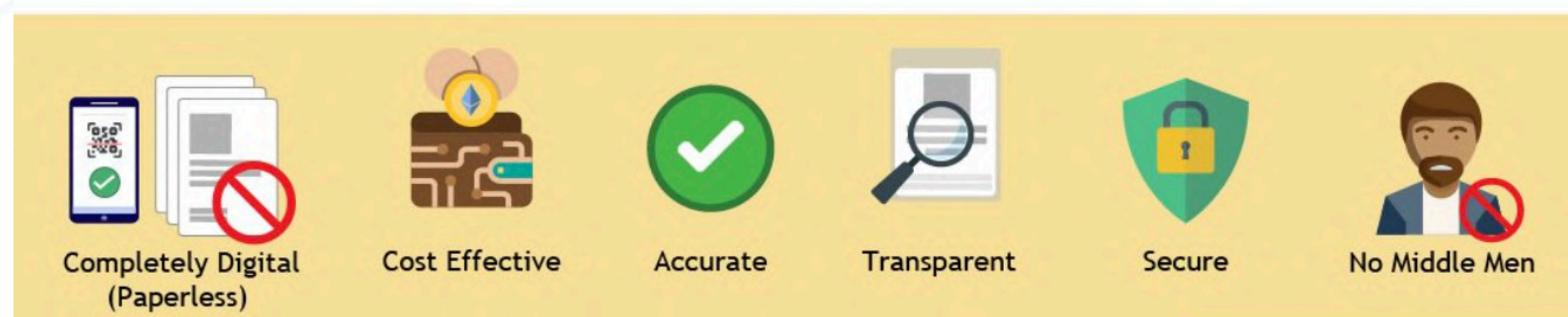
How do they work?

Smart contracts operate on a blockchain by executing basic “if..then..” clauses written in code. When specified criteria get fulfilled, respective activities are performed. These criteria may include transferring #money to the relevant parties, registering a vehicle, delivering notifications, or issuing a ticket. When the transaction is completed, the blockchain is updated.



Benefits:

- Speed, efficiency, and accuracy
Because smart contracts are automated, and there is no paperwork to complete, no time is wasted correcting mistakes that may occur when filling out forms manually.
- Security
Blockchain transaction records are encrypted, making it difficult to hack. Also, since each record on a distributed ledger is linked to the preceding and subsequent entries, hackers would have to modify the whole chain to alter a single entry.
- Transparency and Savings
Since there is no intermediary involved, the associated fee gets saved. No involvement of a third party creates trust in the system.



LAUNCHING A DAO



@vedangvatsa

A decentralised autonomous organisation (DAO) operates without the need for hierarchical management and can serve a variety of objectives. These groups can create freelancer networks where contracts pool their funds to pay for software subscriptions, philanthropic organisations where members approve payments, and venture capital businesses run by a group. A DAO can be joined in a number of ways, the most common of which is through the ownership of a token.

Smart contracts, which are essentially bits of code that execute automatically when a set of criteria is met, are used by DAOs. Smart contracts are now used on a variety of blockchains, while Ethereum was the first to do so. The DAO's regulations are established by these smart contracts. Those who own a share in a DAO are given voting rights and have the ability to influence how the company functions by voting on or proposing new governance proposals.

This methodology protects DAOs from being overwhelmed with requests by requiring that a

proposal be approved by a majority of stakeholders. The method for determining that majority varies from DAO to DAO and is described in the smart contracts.

DAOs are completely self-contained and transparent. Anyone may see their code because they are built on open-source blockchains. Because the blockchain records all financial transactions, anyone may audit their built-in treasuries. A DAO is typically launched in three stages:

- Making a smart contract: To begin, a developer or group of developers must create the DAO's smart contract. They can only amend the rules specified by these contracts through the governance system after they launch. As a result, they must thoroughly test the contracts to ensure that essential aspects are not overlooked.
- Following the creation of the smart contracts, the DAO must decide how to acquire financing and how to implement governance.

Tokens are frequently sold to raise funds; these tokens grant holders voting rights.

- The DAO must be launched on the blockchain once everything has been set up. Stakeholders will now make decisions on the organization's future. The founders of the organization — individuals who developed the smart contracts — no longer have any influence over the project more than the other stakeholders.

DAOs offer significant advantages over traditional organisations since they are internet-native. The lack of trust required between two parties is a significant advantage of DAOs. While a typical organisation demands a great deal of faith in the people who run it — particularly on behalf of investors — DAOs just require trust in the code. It's easier to trust that code because it's open source and can be thoroughly tested before being released. After a DAO is started, every action it performs must be approved by the community and is totally public and verifiable.



NFT

Back to basics



- **Fungibility**

Fungibility refers to the ability of an asset to be replaced or exchanged. A fungible asset may be replaced or exchanged for another indistinguishable portion.

- **Non-fungibility**

It is the polar opposite of fungibility, something that is one-of-a-kind and irreplaceable. A non-fungible item cannot be readily replaced, such as an autographed book or a rare antique coin.

Non-Fungible Tokens

An NFT is a Non-Fungible Token (a one-of-a-kind digital token), which many people regard as a certificate of authenticity, or a deed or evidence that you have the right to show the aforementioned art on your wall or in your wallet (digital wallet).

It may provide you ownership of the copy you purchased, but not necessarily ownership of the original artwork. Unless otherwise specified in the contract, the creator automatically retains the copyright. In any case, non-fungible implies 'irreplaceable,' since each token is unique. And 'unique' produces scarcity, which raises the market value of NFTs.

NFTs have received a lot of interest in the area of art and entertainment. However, with the rise of Web3 and the Metaverse, rising consumer demand for virtual assets, and a move toward the concept of digital ownership, NFTs find a use case that is beyond just art. We're beginning to see it grow into music, entertainment, sports, and live events, providing value and usefulness that goes beyond just being a digital collection.

While the technology is still in its early phases, possible real-world uses for NFTs might include:

Ensuring authenticity and transparency: Imagine a future in which you can scan a QR code on a product you purchased online and witness its supply chain history. With further instruments, you can look around for data about carbon credits and even donate directly to the families of the workers.

Real estate: NFTs may be used to transfer land titles, establish evidence of ownership, and even monitor property value fluctuations over time. The fractional ownership model is already being piloted by several startups across different geographies.



Non-Fungible Tokens

Verified Vehicle History: NFTs have the potential to be the auto industry's answer to manipulated car history records. By incorporating NFTs and blockchain technology into their automobiles, future purchasers will have complete transparency into a vehicle's past and will be able to make a more confident used car purchase.

Ticketing: NFTs can address concerns of fraud in ticketing, whether for concerts, sports events, or airline tickets.

Why (and how) NFTs hold value:

IP: NFTs often provide the possessor with a set of privileges. Common NFT rights include the ability to exhibit or edit art, get access to unique content, and transfer or sell your rights. This adds value to holders who can create an online presence around the art, potentially increasing the value of the underlying art and any linked NFT collection.

Communities: To attract members to a community, you must first create a compelling value offer. If you do this well, you will create a tribe of brand ambassadors and champions who will promote the value of your collection to their network of prospective consumers and dedicated followers.

Exclusivity: NFTs are unique. As a result, they are ideal for highlighting characteristics that are unique to their owners. NFTs, for example, may be used to determine who has access to particular areas of a property (clubs? or even a portion of any website). In other words, they may act similarly to a membership card.

Underwriting: Underwriting is the procedure through which a person or organization assumes the financial risk in exchange for a fee, thereby storing value for an interesting upcoming project. You will be able to pick whatever NFT collection you want to insure as an underwriter by putting ETH into that collection's unique underwriting pool.





Citizens of the Metaverse

There is a limitless chance to expand the metaverse since it is as limitless and wide as our imagination allows us to imagine it.
In the next 3-5 years, estimations of the metaverse's market worth vary from \$250 to \$800 billion USD, depending on its many aspects. (Source: [OlyverWymanForum](#))

Metazens

#CollegeEducated #Millennials #Gen Z #Urban #Males #RiskTaking #DataAgnostic #Memes

- Consider metaverse a place where they will be free to play, have fun, and explore independently
- Lack **creativity** in what they expect from the metaverse
- Willing to pay for experiences that involve **gaming, socializing**, and working
- Interested in **experiences** specific to the metaverse, such as virtual events, simulations, and digital objects
- Invest in **cryptocurrencies** at 3X the rate of the general population, and 5Xs as much in **virtual real estate** and in **NFTs**
- See the volatility of virtual assets as an opportunity to win big
- More likely to use Instagram, TikTok, and Snapchat



@vedangvatsa



GenZ's Metaverse Starter Pack



Roblox

(darling of the metaverse)

- Roblox has recently become the darling of the metaverse. Roblox, a platform where users can play millions of 3D online games, personalise their avatars with skins, and spend/earn Robux, is said to be used by half of the American youngsters.
- Roblox also boasts the most monthly active users (202 million as of April 2021) and the most daily engagement among the newer metaverse platforms (nearing 50 million DAUs as of December 2021).
- Roblox is a closed environment, which means that avatars and skins created inside the game can't be used outside of it. It's a platform that relies on user-generated content, with 1.3 million developers earning Robux (in-game cash) as of October 2021, with these creators on course to make \$500 million from their gaming creations this year.
- Roblox is one of the most valuable firms in the metaverse, with a market worth of \$61 billion dollars, and is still in the early stages of generating value from brands, franchises, and artists on their platform.

Sandbox

(real estate and stuff)

- The Sandbox is a virtual environment built on the Ethereum blockchain in which gamers may create, control, and monetize their gaming experiences. Corporations, celebrities, and people are staking their claim inside the metaverse via NFT-based real estate plots (two-thirds of which have already been sold).
- The Sandbox has approximately 12,000 virtual property owners and has sold over \$144 million in gross merchandise value for its land as of November 2021 (including 165 brands, and more than 500k registered wallets).
- Softbank's Vision Fund has invested \$93 million in the startup, with plans to expand "beyond gaming into industries such as fashion, architecture, virtual concerts and performances, art galleries, museums, and more."
- The Sandbox is using a "play-to-earn" strategy to reward gamers for their time spent in the metaverse, and it's creating an open metaverse to allow for more cooperation between artists and brands.

Axie Infinity

(NFT-based video game)

- Axie Infinity is a game that explores the notion of bringing crypto to the masses via gaming.
- Players acquire NFTs of charming creatures called Axies and fight them against one other in Axie Infinity, a blockchain-based game built on Ethereum (+ Ronin side chain to decrease fees and transaction times).
- Axies may be traded for real money in the game's marketplace (some selling for more than \$600k), and they can also be bred to produce more NFTs.
- You'll need at least three Axies to participate in this "play-to-earn" concept, and they're now available for as cheap as \$70 on Axie's marketplace as of December 2021.
- To put the amount of activity going on inside Axie Infinity in perspective, it's the most successful blockchain-based game to date and the biggest overall NFT project in terms of trade volume (with \$341 million in transaction volume on its marketplace in the past 30 days, as of Dec. 27th).

Decentraland

(metaverse's promise)

- Decentraland is an Ethereum-based application that aims to encourage a worldwide network of users to govern a shared virtual space.
- Users of Decentraland may explore, engage, and play games in this virtual environment while buying and selling digital real estate. Users may now utilise interactive applications, in-world payments, and peer-to-peer communication thanks to the platform's evolution.
- In Decentraland, operations are governed by two sorts of tokens:
 - LAND — A non-fungible token (NFT) that is used to define the ownership of digital real estate land parcels.
 - MANA — A cryptocurrency that may be used to buy LAND and other virtual products and services in Decentraland.
- Changes to the Decentraland platform are made possible through a network of blockchain-based smart contracts that enable MANA owners to vote on policy modifications, land auctions, and new development subsidies.



Case Study

Meta (formerly Facebook)

- **Infrastructure for data centres**

Meta has spent \$21.3 billion on 14 data centres in the United States and \$4.1 billion on four data centres across the world during the last decade. Tom Furlong, Meta's President of Infrastructure & Data Centers, claimed that the company has 48 operating facilities and another 47 under development.

- **Additional versions of VR and AR products and content**

Facebook bought Oculus for \$2 billion in 2014, marking the company's first push into virtual reality. Meta spent \$250 million on VR content between 2014 and 2016, and has committed another \$250 million to future content initiatives. During the 2017 Connect event, CEO Mark Zuckerberg said that the company aims to spend \$3 billion or more on virtual reality products over the next decade. Meta also bought six virtual reality content companies in the last two years.

- **Recruiting top talent**

As of March 31, 2021, about 10,000 Meta workers were working on expanding the company's augmented and virtual reality operations, accounting for almost a sixth of the total workforce. It also plans to hire an additional 10,000 workers in Europe for its Facebook Reality Labs division.

- **Responsibility**

Meta intends to spend \$50 million across many worldwide collaborations over the next two years in order to ensure that Metaverse-related goods are produced responsibly. Meta has announced 18 collaborations to date, all of which are aimed at assuring accountability in a few critical areas: economic opportunity, privacy, safety and integrity, and fairness and inclusion.

- **Creators of content**

Meta launched a \$150 million fund to assist, educate and nurture the next generation of creators during the 2021 Connect event. These initiatives will specifically target Metaverse producers' skill sets, high-quality training material, worldwide access to Meta technologies, and responsible research. It has a \$150 million VR/AR learning fund for creators. These funds will be distributed via community contests with prizes of up to \$10,000 for the top three winners, and its Creator Accelerator Program, which will debut in early 2022.

A decorative graphic of several light green leaves on a stem, positioned on the left side of the slide.

\$13 trillion

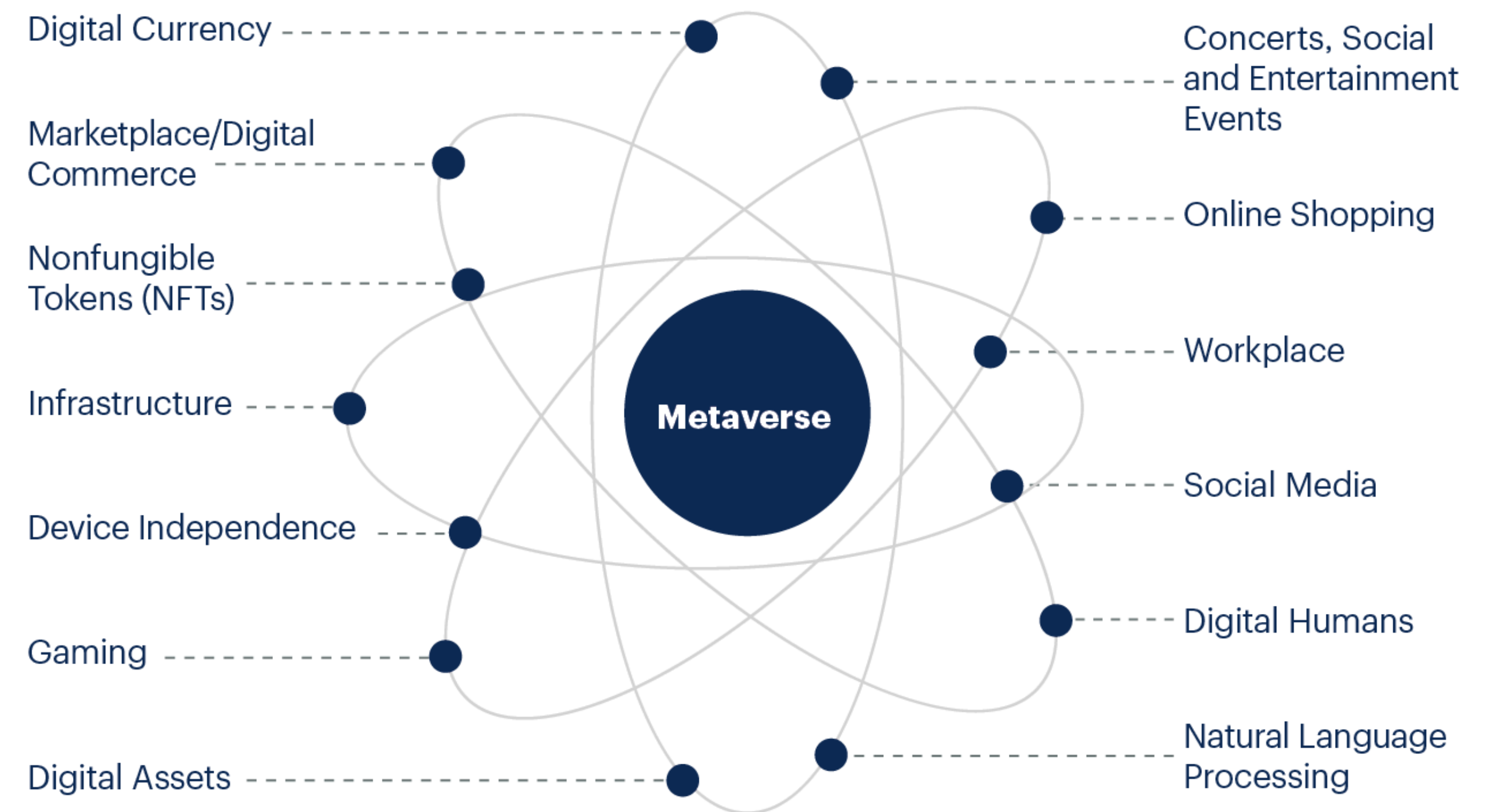
could be Metaverse's economy by 2030, according to Citi

According to [Gartner](#), it is expected that by 2026, 25% of people will spend at least an hour per day in the **Metaverse**

Activities, like the following, can someday be brought together in a single Metaverse, such as:

- Shopping accessories for your digital avatar
- Virtual real estate
- Virtual office meetings
- Immersive commerce
- Virtual classrooms
- Virtual events and gatherings
- Digital art and collectables
- Customer support
- Advertisements
- Gaming
- Dating

Elements of a Metaverse



gartner.com

Source: Gartner
© 2022 Gartner, Inc. and/or its affiliates. All rights reserved. CTMKT_1635001

Gartner®

Your identity in the Metaverse

Privacy is a fundamental human right and a prerequisite for full self-expression and autonomy. Total anonymity is not always practical for a functional society since evidence of ownership and right of access need some kind of identification and/or reputation (and social score?). On the other hand, pseudonymity allows for the right to privacy for one's true self while also allowing for the "right to access". Separation of identities between our true selves, our social selves, and our working selves may afford both privacy and access.

Individual autonomy as well as the advancement of society as a whole, are harmed by the absence of privacy. Consider a surveillance state where citizens are afraid of being persecuted, imprisoned, or worse, physically injured if they voice opposing viewpoints.

Authoritarian regimes have a history of instilling fear in public, preventing citizens from freely expressing their opinions, going to the streets in protest, and propagating alternative views. This may be observed in areas like academics and businesses. Many scholars, for example, will be influenced by their superiors and will only push back - out of fear of retaliation or exclusion from their field.

Autonomy

The "right to access" is essential for a functional society, just as privacy is required for an open society. The capacity to verify one's ownership of a valuable asset, credential or even clearance to certain digital and physical areas is understood as the right to access. Individual autonomy requires the ability to access and verify ownership. The capacity to verify property ownership, for example, must be linked to a particular person. There would be no way to correlate property ownership between two apparently similar persons in an anonymous setting.

The right to access also applies to how we handle our finances and bank accounts. Our individual worth would be open to any anonymous actor if we don't have the capacity to show ownership. The capacity to show citizenship to governments is another example. Most individuals in today's society have passports from certain countries that allow them to travel across borders.

Being "undocumented," or not having evidence of nationality, is not the same as being stateless, although a lack of identifying papers such as a birth certificate might lead to statelessness.

It should be feasible to protect one's fundamental human right to privacy while having the ability to access information and verify ownership. This is accomplished via numerous degrees and kinds of identification, which have been made much more accessible thanks to distributed networks and modern technology. What if a single person or organisation could establish and maintain various pseudonyms that granted access to different things?



Naval

@naval

The metaverse isn't a 3D world owned by some corporation.

It's a permissionless market-network which respects and interconnects all user-owned and cryptographically-secured digital identities, reputations, wallets, communities, spaces, and objects.

It's bootstrapping right now.

September 5th 2021

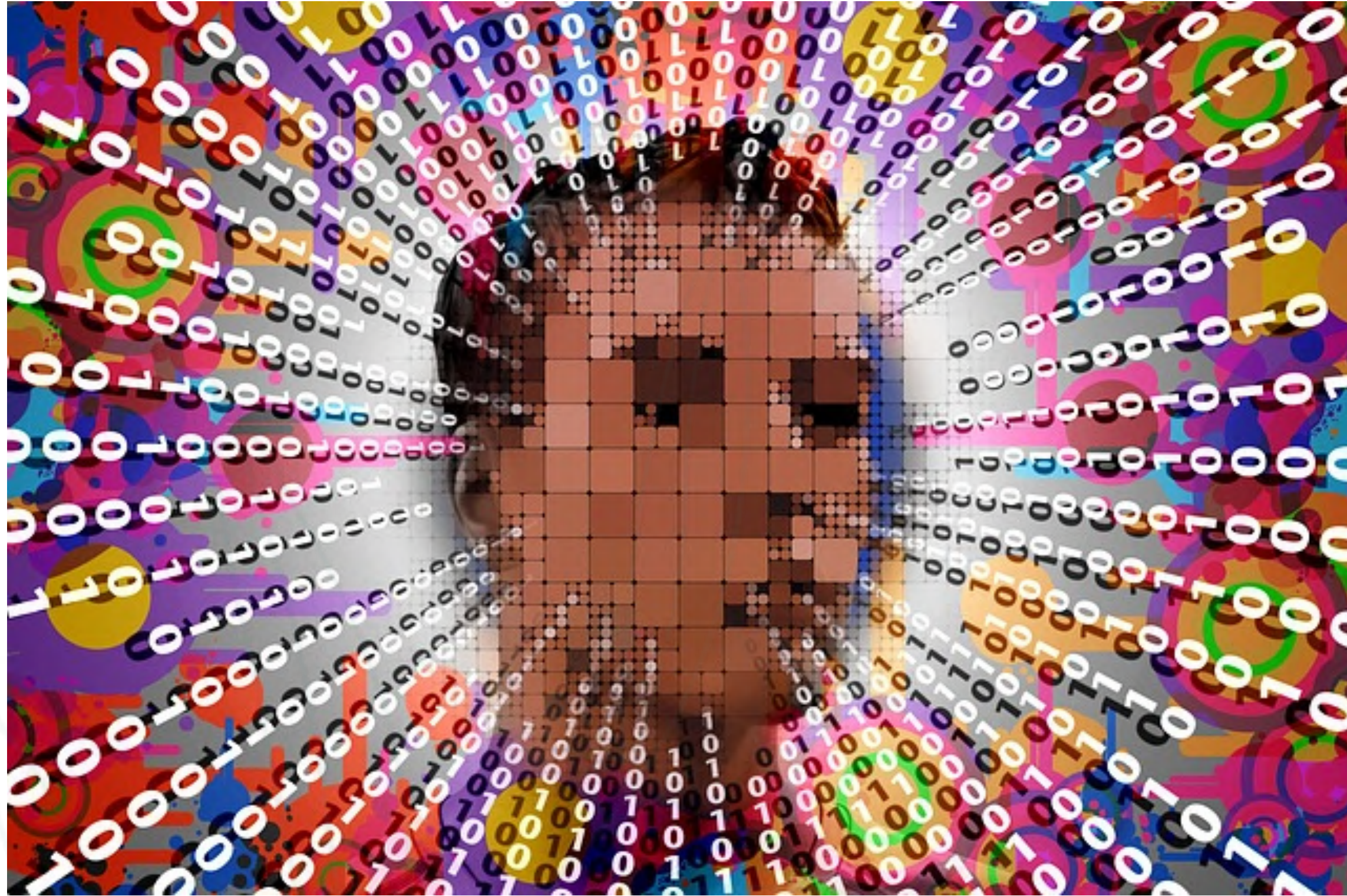
Pseudonymity

Pseudonymity is a key aspect of the metaverse, where identity is based on avatars, digital assets, and activities rather than physical presence. All avatars start off with complete pseudonyms. The individual who adopts the avatar might stay completely anonymous or link portions or all of his identity.

Let us talk about Twitter, which is like a play-to-earn game. Those who thrive at this game gain influence, valued in both monetary and power terms. Twitter's digital asset is its follower count. The number of followers is similar to a bank account filled with non-fungible, non-tradable tokens that generate interest via influence and, eventually, money.

Players can only win the Twitter game by mastering the game's mechanics - providing amazing content — not by relying on genetic advantages. A pseudonym's selected characteristics may not guarantee exceptional material or even attention.

Arvind Narayanan's concept of [33 bits of Entropy](#) is an excellent way to explain degrees of pseudonymity. With 7.5 billion individuals on the planet, determining a person's identity requires just 33 pieces of information. There are only 7.5 billion people on the planet, thus 2^{33} equals 8.6 billion. As a result, you can de-anonymize someone using 33 bits of independent data. You know who they are if they have 0 pieces of anonymity left. They are 1 out of 2^{10} or 1 out of 1,024, with 10 bits of anonymity remains.



Identity

That is acceptable to the majority of people in developed nations. They have great prestige all around the globe because of their identity. You may travel freely anywhere in the world if you hold an American passport (with some exceptions).

Of course, you may always travel to another nation and acquire a new ID, but your true identity will always stay the same. It is unchangeable. You don't have control over your own identity!

When you attempt to define identity, the difficulty becomes evident. What exactly is identity? Is it something you're born with or choose to have?

You were born with a body that you will never be able to get rid of. However, your mind is constantly changing, and you have control over how you think. When you define identity as your intellect and a collection of ideas, you begin to see that your identity is always changing. You make decisions about who you are and who you want to be throughout your life. Your physical self, on the other hand, will never change.

You may actively change your spiritual identity in the actual world, but not your physical one. Governments provide you with identification. In other words, nation-states confer your identity on you. Your mind, body, and identity are three distinct entities in the metaverse. You have complete control over all of them. You have the freedom to select who you want to be and how you want to appear.

You pick your identity in the metaverse!



Reese Witherspoon ✓

@ReeseW



In the (near) future, every person will have a parallel digital identity. Avatars, crypto wallets, digital goods will be the norm. Are you planning for this?

10:54 PM · Jan 11, 2022



People are still evaluated in the real world based on their skin colour, gender, and other factors. This is not the case in the metaverse, where you have the freedom to select your own identity. We are solely rated in the metaverse depending on our output. The quality of our work is crucial!

We create a work atmosphere devoid of bigotry, prejudice, and bias by not exposing our real-world identities and instead employing avatars.

Pseudonymity in Crypto

Many people in the crypto community use pseudonyms for privacy reasons, either to conceal their true identity as part of a drive toward self-sovereignty or to protect their privacy and security. Bitcoin appeals to many people because pseudonymity is built into the system.

When you create a bank account, you must provide identification that connects your financial activities to your identity and is neither anonymous nor pseudonymous. When you make a Bitcoin wallet, you generate an alphanumeric address that enables you to send and receive bitcoin and is publicly viewable on the blockchain to the rest of the world. However, since financial forensics on your public address may be connected back to your real-world identity, this address offers pseudonymity rather than anonymity. The discussion between privacy activists and policymakers over the benefits and drawbacks of pseudonymous and anonymous cryptocurrencies is continuing, but given the rapid pace of technological advancement and widespread acceptance of crypto, a consensus should be reached soon.

Technologies powering metaverse

Cryptography and Blockchain

Enterprises may use blockchain to create decentralised and transparent systems that provide digital evidence of ownership, collectibility, and value transfer. Cryptocurrencies serve as a means of trade for users to exchange value while exploring and interacting in the 3D virtual world. Gamers in popular games like Decentraland, for example, need local digital currency MANA to acquire virtual land and other game accessories in order to continue playing. People that contribute to the growth of the Metaverse ecosystem are likely to be rewarded with cryptocurrency, similar to how miners are compensated.

Artificial Intelligence

AI has a broad range of applications in our daily lives. Similarly, AI has made it possible to create immersive virtual environments. AI is bringing value to Metaverse in a variety of ways, regardless of the project type. AI can analyse 3D scans and photos to create more lifelike avatars that match the actual person while also enriching the visual details for a game. AI can analyse 3D scans and photos to create more lifelike avatars that match the actual person while also enriching the visual details for a game.

Augmented Reality and Virtual Reality

Metaverse relies on AR and VR to provide users with an immersive 3D experience. Presently, AR-based apps enable users to perceive their environment via engaging digital images similar to those found in games like Pokemon GO. Users may explore a fully computer-generated digital environment using VR headgear, gloves, and digital sensors.

Internet of Things

IoT system connects our physical environment to the internet by allowing data to be sent and received through sensors. It receives data from the actual world and converts it to virtual space, improving the accuracy of digital representations. IoT data streams can predict how things in the Metaverse will behave depending on the changing surroundings and other factors. It can leverage AI and ML to precisely manage the data it collects to improve the Metaverse ecosystem.

5G

Because AR requires 5G to minimise latency, and 5G (by transferring computation to the cloud) might reduce processing and battery requirements in the device, making it lighter, cheaper, and last longer, 5G is a significant driver of Metaverse adoption.

Decoding Buterin's concept of Soul-Bound Tokens

Soulbound tokens (SBT) are non-transferable, publicly verifiable digital tokens that may serve as a form of CV for web3 users, displaying a person's memberships, credentials, and affiliations.

In their whitepaper, Glen Weyl, Puja Ohlhaber, and Vitalik Buterin characterised SBTs as a way to "eschew today's hyper-financialization" of the web3 ecosystem in order to transition to a Decentralized Society "encoding social relationships of trust."

Unlike NFTs and other cryptocurrencies, which may be sold on the open market and moved from one wallet to another, soulbound tokens, as the name suggests, are permanently bound to a wallet or account for the duration of their existence. So-called "Souls" are wallets or accounts that house soulbound tokens.

Consider a blockchain account (Soul) that maintains immutable data such as academic credentials, job history, or works that document a person's experiences. SBTs, like a CV, may aid in the development of a user's digital reputation across web3 solutions.

However, their entire potential can be seen when one Soul may issue an SBT to another Soul (which can be proved by other Souls), implying that a community might be a Soul that issues

SBTs to natives or a corporation that provides SBTs to shareholders.

Furthermore, an individual or corporation may be a Soul that recommends a person after successfully doing business with them. This notion enables a soul to demonstrate integrity, trust, affiliations, and credibility, allowing web3 networks to be formed on provenance and reputation rather than money-oriented structures.



Decoding Buterin's concept of Soul-Bound Tokens

Why and why not?

The tokens have additional functions apart from representing our unique information and making it tough for fraudsters to mimic us. They might be used for event tickets, unique airdrops (also known as "Souldrops"), and other community-specific perks. For example, a company may simply send out reunion tickets to all alumni who graduated within a certain time period.

Of course, the inverse is true as well.

Bad actors might utilise SBTs to identify, target, and damage members of certain groups. The possibility of regulating entities is especially concerning. Holders of a given SBT, for example, may be denied access to facilities, denied medical treatment, rejected travel permits, and have their voting rights taken away, among other things.

In their study, the authors of the whitepaper admit this dystopian possibility, saying that a database of SBTs may be used to "automate redlining of disfavored social groups or even target them for cyber or physical attack, enforce restrictive migration policies, or make predatory loans."

What's the point?

Every human connection or commercial transaction is reliant on stakeholder trust, however, web3 is hampered in this area due to the high degree of privacy and anonymity in web3 protocols. As a result, web3 protocols have become increasingly dependent on the centralised architecture of web2, which they are designed to replace. For instance:

- DAOs depend on web2 platforms like Discord to avoid Sybil attacks.
- OpenSea is used by NFT collectors to demonstrate the provenance of their acquisitions.

Soulbound tokens might be the missing link in web3's trust bridge. Because of their non-transferability, they may be used to establish social identities that allow protocols and persons to rely on trust while protecting privacy.

Jack's Bitcoin-backed decentralised Web5

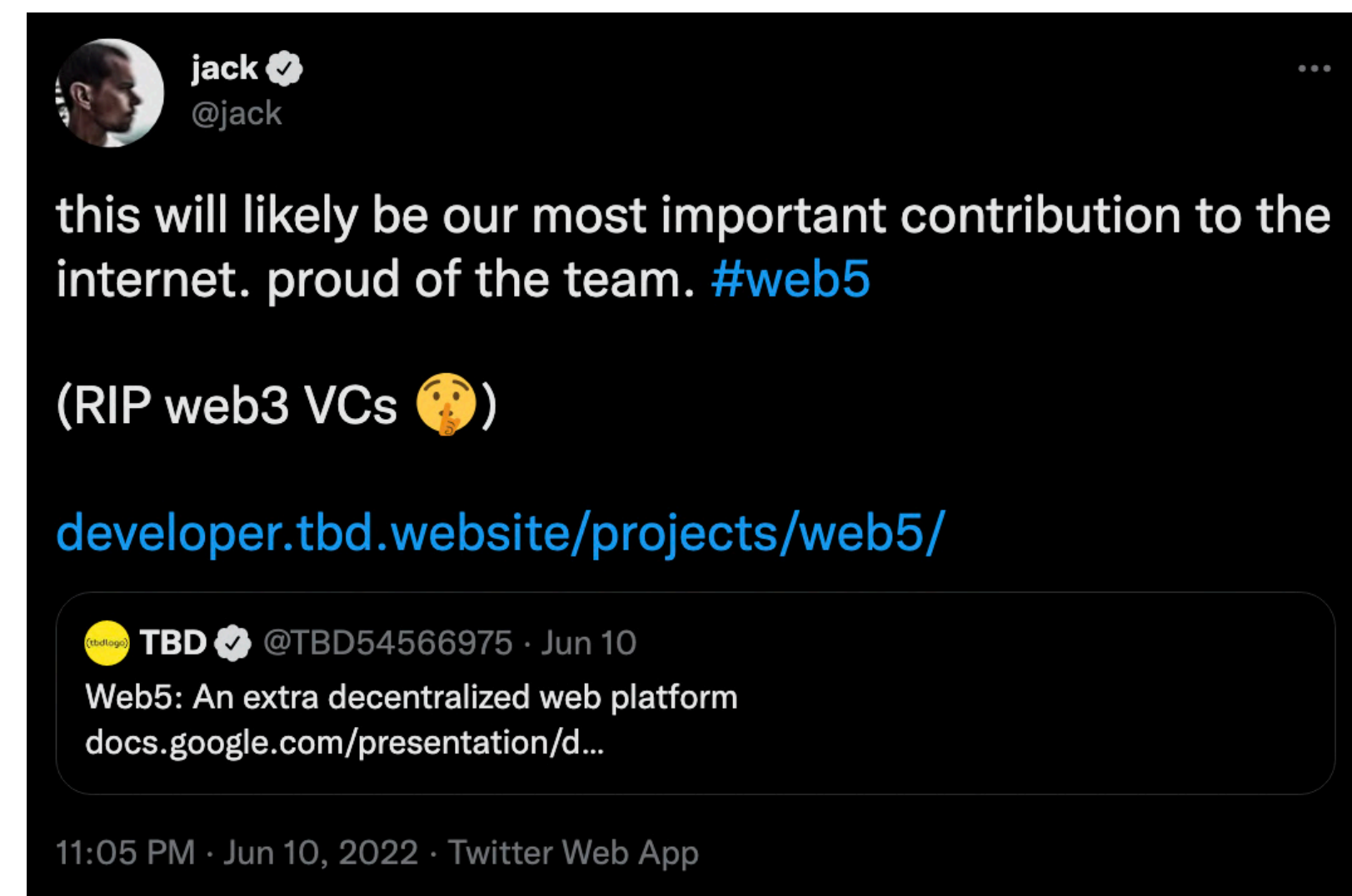
TBD, Jack Dorsey's Bitcoin-focused business arm and a subsidiary of Block Inc., revealed recently that it is developing a new decentralised web: Web5.

Web5 is predicated on the belief that Web3, the concept of creating a decentralised web utilising blockchain technology and cryptocurrencies, has good intentions but employs the wrong tools.

Web5 uses Bitcoin, the decentralised monetary network, plus a slew of technologies to establish a new ecosystem of decentralised identities, data storage, and apps in which the users have ownership over their personal data.

Decentralized innovations on the internet over the last several decades, such as BitTorrent, have shown that blockchain technology may not be required for decentralisation. Rather, the blockchain has been believed necessary for: mitigating the double-spend issue in order to effectively transfer peer-to-peer money with Bitcoin.

Web5 from TBD is comprised of software components and services such as decentralised identifiers (DIDs), decentralised web nodes (DWNs), self-sovereign identity service (SSIS), and a self-sovereign identity software development kit (ssi-sdk). These components allow developers to concentrate on creating user experiences while allowing decentralised identification and data storage in apps more effortlessly.



Jack's Bitcoin-backed decentralised Web5

What exactly is Web5?

TBD, Jack Dorsey's crypto company, recently announced the introduction of Web5. According to their official website, the objective is to create an additional decentralised web that puts you in control of your data and identity.

According to the official website:

“The web democratized the exchange of information, but it's missing a key layer: identity. We struggle to secure personal data with hundreds of accounts and passwords we can't remember. On the web today, identity and personal data have become the property of third parties.

Web5 brings decentralized identity and data storage to your applications. It lets devs focus on creating delightful user experiences, while returning ownership of data and identity to individuals.”



Web5's mission is to produce a one-of-a-kind collection of tools built on Bitcoin that will transform the financial system as we know it. This would enable investors and people to preserve and own their data and maintain control over all of their relationships.

One of the primary differences between Web5 and Web3 platforms is that Web 3.0 platforms are often more centralised in terms of what users believe, despite marketing attempts to the contrary. According to Jack Dorsey, Web 3.0 technologies are built on single point of failure systems, citing Solana (SOL) and Ethereum as examples (ETH).

As a result, a system based on Bitcoin's decentralised structure and absence of single points of failure may be more suited to the principles advanced by Web 3.0 enthusiasts.

Self-owned identities that allow decentralised identity authentication and routing, verifiable credentials as data formats and models for cryptographic presentation and claim verification, and decentralised web nodes are among the Web5 pillars.

Jack's Bitcoin-backed decentralised Web5

The Pillars of Web5

It is too soon to consider Web5 replacing Web 3.0. Indeed, it may be long before we see the true consequences of what Web5 wants to accomplish. At present, this is only a notion and a proposal that might be supported and modify many of the things we thought were “normal,” such as centralised blockchain networks.

However, things are changing. Many concerns have harmed the bitcoin market's reputation, including developing initiatives that advertised decentralised solutions but ended up being centralised platforms with single points of failure.

We are presently transitioning from Web2 to Web3. It may take some time before we witness a transition from Web3 to Web5. Web2 might possibly be divided into Web3 and Web5, providing new chances for developers, businesses, and people to choose which version of the internet would work best.

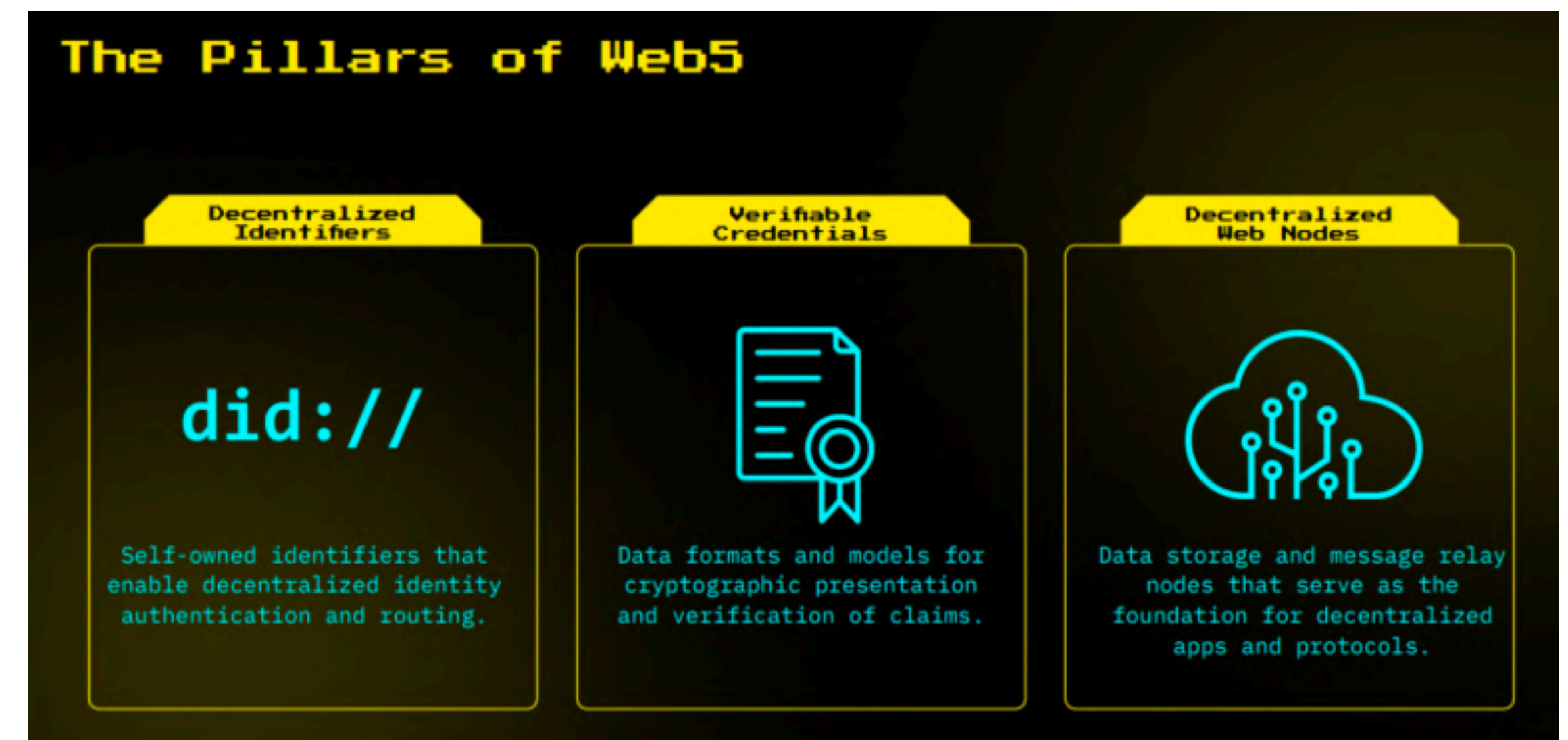
The Proposal of Jack Dorsey

Jack Dorsey's TBD proposal is associated with a distinct approach to how Web3 should function. Rather than depending on many protocols and potentially controlled blockchain

networks, we may be going toward Web5, which is built on Bitcoin and its immutability and decentralisation.

One of the key features of Web5 is the use of Decentralized Identifiers (DIDs), which might depend only on the Bitcoin blockchain. There is no need to build a new network of validators or solutions; everything that is required can function on top of Bitcoin.

As a result, we can see that Jack Dorsey's Web5 proposal is a true self-sovereignty solution that operates and depends on Bitcoin. There is no need for an extra consensus process or network.





Central Bank Digital Currencies

Different governments are motivated to research and trial the implementation of CBDC for a variety of reasons, including to improve payment system efficiency, minimise payment system risks, increase access to financial services (financial inclusion), and improve cross-border payments.

Bahamas Sand Dollar

- The Bahamas' geography is dispersed, with pockets of low population and several remote island villages with minimal or no access to physical means of delivery. Only electronic channels are accessible for the services. Furthermore, in response to increased operating expenses, the banks' branch network has been reduced.
- Around 90% of Bahamians possess cellphones with mobile wallet capability as of 2017. The Bahamas planned to modernise the payments system's infrastructure. This prompted the Central Bank of the Bahamas to initiate the Sand Dollar project's trial phase in December 2019.
- The CBDC was envisioned as the glue that would tie different payment systems together when the initiative began with very little activity on digital and mobile payments.

Singapore's Project Ubin

- Singapore has modern payment systems, and banks service the bulk of the population. Singapore has a high smartphone penetration rate of 78%. Excellent mobile and fixed internet infrastructure help to enable this.
- Singapore has one of the greatest internet penetration rates in the world, with 91% coverage throughout the city-state.
- The Singapore Monetary Authority (MAS) found that an international settlement network might allow quicker and less expensive transactions than traditional cross-border payment routes. As a result, MAS launched Project Ubin²⁶. The study investigated the use of CBDCs to establish a multi-currency payment platform. MAS has worked on this initiative with other nations, like Canada and Thailand, to test CBDC cross-border payments.

Bank of England

- Given that the usage of banknotes is declining in England while the use of privately issued money and other payment methods is increasing, the Bank of England (BOE) is looking at the possibility of CBDC.
- BOE aspires to deliver a safer and more trustworthy form of money to consumers, companies, and the financial system as an alternative to privately produced digital money.
- In June 2021, the BOE issued a CBDC discussion paper in which it requested public input and suggestions to aid in the evaluation of CBDC for future deployment.

Sweden's e-Krona

- Sweden has one of the world's most sophisticated digital economies. Cash use has decreased dramatically in Sweden over the last decade, raising worries about access to government-backed money as well as the safety and effectiveness of the domestic payment system.
- In Sweden, 90% of all payments are done via digital means, according to Riksbank (the central bank). Furthermore, the majority of payments in Sweden are made via third-party payment service providers (PSPs) such as Swish.
- Sweden is responding by attempting to establish a retail digital currency to replace Swish, a digital payment programme created by six Swedish banks. This will try to avoid systemic risks while also asserting the central bank's currency's autonomy.

Canada's Project Jasper

- The Bank of Canada (BOC) is now focusing on the usage of CBDCs as a supplement to banknotes.
- The CBDC is being created as a backup plan, given that any solution would take a long time to design and implement.
- The growth of alternative digital currencies and the fall in cash use are two plausible explanations for the required effort, according to BOC.

BIS's Project Dunbar

- The Bank for International Settlements Innovation Hub, the Reserve Bank of Australia, Bank Negara Malaysia, the Singapore Monetary Authority, and the South African Reserve Bank collaborated in September 2021 to explore the usage of CBDCs issued by various central banks for international settlements.
- Project Dunbar intends to create prototypes for shared multi-CBDC platforms that would enable financial institutions to deal directly with one another in digital currencies issued by participating central banks, bypassing middlemen and reducing transaction time and cost.

China's Digital Yuan

- The People's Bank of China (PBOC) started creating and testing a digital fiat currency called the digital Yuan in 2017.
- The Digital Yuan is a retail CBDC aimed at updating China's domestic payment system to fulfil the public's everyday payment demands, increase the efficiency of the retail payment system, and lower retail payment costs.
- China began the second phase of its planned digital Yuan deployment in September 2021, with the goal of making digital Yuan accessible to overseas tourists during the 2022 Beijing Winter Olympics.
- The Chinese government is using the 2022 Winter Olympics in Beijing to boost digital Yuan experiments.

Digital Turkish Lira

- The Central Bank of the Republic of Turkey (CBRT) has begun testing and developing a prototype for a Digital Turkish Lira.
- The research will also look at how blockchain technology may be integrated into payment systems.
- The CBRT emphasised that the pilot project is just a test and does not imply that a digital Turkish Lira would be issued. The findings will be made public this year.

US's Federal Research on CBDC

- The US Federal Reserve issued a discussion paper analysing the costs and advantages of issuing CBDC in January 2022, with the goal of soliciting public feedback on the issue of a US CBDC.
- According to the preliminary findings of the US Federal Reserve, a prospective US CBDC would best serve the interests of the US by being privacy-protected, intermediated, widely transferrable, and identity-verified.
- While a CBDC might offer a secure, speedier, and digital payment alternative for homes and companies as the payments system evolves, there may be drawbacks, according to the report. They include how to ensure that a CBDC maintains monetary and financial stability while also complementing conventional payment methods.

India's Digital Rupee

- India's digital Rupee: India announced the introduction of a digital version of the rupee in 2022 at its annual budget presentation on February 1, 2022.
- It is expected to give a big boost to India's digital economy and will also lead to a more efficient and cheaper currency management system.



Some of the Best Performing Cryptocurrencies of 2021

Shiba Inu (SHIB)

- The self-proclaimed "Dogecoin Killer" had a spectacular year in 2021, with a price rise of 43million% from January to December.
- At the start of the year, it was worth \$0.00000000000077. The coin did not excite the curiosity of many people at the time. However, a resurgence in May provided Shiba Inu with a much-needed lift, allowing it to solidify its position.
- In October, the currency reached an all-time high of \$0.00008616 and a market capitalization of \$40 billion. Shiba was trading at \$0.00003407 at the end of December.

Terra (LUNA)

- Luna, too, had a stellar year in 2021, with gains of 13,790%. It began the year at \$0.65 and surged to a new high of \$22 in early March.
- Then, in the second part of the year, it hit an all-time high of \$81 in early December.
- It had broken the \$100 barrier by late December, reaching an all-time high of \$103.33 before closing at \$85.49.

Axie Infinity (AXS)

- At the start of 2021, AXS was trading at \$0.53. When the focus turned to the gaming sector in June, this utility coin gained traction.
- The token used in Axie Infinity, a Pokemon-inspired play-to-earn metaverse game based on the Ethereum blockchain, reached an all-time high of \$164 in November before falling to \$94.90 in Jan 2022.
- During the year, its value increased by 12,022%.

Solana (SOL)

- In 2021, Solana increased by more than 10,000%. The coin started the year at \$1.52 and by mid-May had surpassed the \$50 milestone.
- In August and September, the price soared from \$40 to almost \$180.
- In November, Solana hit an all-time high of \$259 per coin. It was worth \$172 in December.

Bitcoin

- Bitcoin, the most valuable cryptocurrency in terms of market capitalization, stayed in first place during 2021, maintaining its lead over Ethereum.
- Prices, on the other hand, fluctuated throughout the year. It reached a low of \$28,803 on January 1 and a high of \$68,789 on November 10.
- Even if the increase was just 138%, it was enough to satisfy investors. Bitcoin was worth \$46,863 at the end of December.



Glossary

Airdrop

A marketing strategy in which cryptocurrency projects distribute their native tokens straight to their customers' wallets in order to raise awareness and acceptance.

Alpha

Important or insider knowledge, notably about the value of digital assets such as cryptocurrencies and NFTs; a measure of an investment's return over and above that of the market or other benchmark.

Altcoin

Formerly used to describe any cryptocurrency that wasn't Bitcoin; however, altcoin is now used to describe any new cryptocurrency with a low market valuation.

Alts

An abbreviation for altcoins.

Ape

Someone who invests significantly in a cryptocurrency or stock, or the act of investing excessively in a cryptocurrency or stock. This might be a response to excitement and FOMO, or it can be done without a thorough understanding of the asset. It's worth noting, though, that this is often a self-assigned phrase with no negative meaning. Is this a Planet of the Apes allusion? Perhaps an allusion to monkeys' incredible physical strength? The beginnings are a little hazy, but one thing is certain: apes work well together.

ATH

Stands for All-Time High (noun) is the highest price ever paid for an asset.

ATL

Stands for "All Time Low" and refers to the lowest price an asset has ever had.

Bear market

A period of fall in a financial market is referred to as a bear market.

Bearish

Refers to having a gloomy opinion of a market or asset's worth, akin to a bear market. If you're bearish on a cryptocurrency, you think its price will fall over time.

Bitcoin

World's first decentralised, peer-to-peer digital money, founded in 2009 by Satoshi Nakamoto.

Block

Collection of transactions that have been published to the blockchain. Every block carries information about the block before it, allowing them to be linked together.

Blockchain

Decentralised digital ledger that allows users to store and transmit data without the need for a central authority. Blockchains are the foundational technology for cryptocurrency systems such as Bitcoin and Ethereum.

Block Explorer

A tool for viewing information on a blockchain, including as transactions, wallet addresses, market caps, and hash rates.

Bridge

A protocol that allows different blockchains to communicate with one another, allowing data, coins, and other information to be transferred.

Bull market

The period in which market prices are increasing.

Bullish

Having an optimistic opinion that a market or asset will grow in price, is akin to a bull market. If you're a Bitcoin bull, you think the currency's value will rise over time.

Burn

The act of withdrawing tokens from a cryptocurrency's circulating supply by transferring them to an inaccessible wallet address is known as burning.

Centralised

A hierarchical organisation in which power and control are concentrated among a small set of decision-makers.

CEX - Centralized Exchange

A cryptocurrency exchange controlled by a centralised firm or organisation: Coinbase, Gemini, and Kraken, for example.

Coin

A cryptocurrency developed on its own native blockchain and designed to serve as a store of value and medium of exchange inside that ecosystem. Ex: BTC, ETH, etc.

Collateral

Any asset that is accepted as collateral for a loan, such as real estate or a digital asset like an NFT.

Cold wallet

A device that stores cryptocurrencies offline. Cold wallets are either physical devices or sheets of paper that carry a user's private keys. Cold wallets are considered a safer way of keeping cryptocurrencies since they are not linked to the internet.

Consensus

The condition of agreement among the nodes on a blockchain. For new transactions to be confirmed and new blocks to be added to a blockchain, consensus is required.

Consensus Mechanism

the mechanism through which nodes on a blockchain agree on a transaction or the network's state. Ref: Proof of Stake and Proof of Work.

Cryptocurrency

A digital asset meant to be used as a means of trade and exchange. Unlike centralised banks or governments, cryptocurrency is borderless, safe, and maintained by blockchains.

DAO - Decentralized Autonomous Organization

An entity that is managed by its users and is built on open-source technology. DAOs are often focused on a single project or objective, and they substitute the old hierarchical processes of legacy organisations for blockchain-based principles.

Dapp - Decentralized Application

A blockchain-based application built on open-source code. Dapps live independently of centralised organisations or individuals, and they often reward tokens to incentivise users to keep them up to date.

Data

Any information entity on the internet, such as name, age, location, interests, browsing history, and so on. Web3 intends to secure this sensitive information and return control to the user.

Due Diligence

Practise of performing your own study before investing in a cryptocurrency, stock, or other asset. It's critical to do your own due diligence rather than relying on what someone else says or does.

Decentralized

A system that runs without the supervision of a central person or authority, instead relying on a peer-to-peer network.

Degen

Derived from the phrase "degenerate gambler." While degen still refers to those who make dangerous bets, it may also apply to anybody who works in the crypto and financial industries. This is a self-assigned word, similar to "ape," and does not have a negative meaning. Degens are proud folks who like trading crazy call options on GME, buying the dip before paying their bills, and aping into shitcoins on occasion.

Decentralized Finance

An ecosystem of peer-to-peer financial instruments based on public blockchains that do not need the usage of banks. DeFi applications are designed to be open and networked, enabling them to work together.

DEX - Decentralized Exchange

A blockchain-based peer-to-peer cryptocurrency exchange. Instead of an intermediate person or centralised organisation, a DEX is managed by its users and smart contracts. Ex: Uniswap, 1inch, Sushiswap, etc.

Diamond Hands

An expression that implies you are highly optimistic on a certain asset and have no intention of selling despite market turbulence.

Difficulty

The amount of computational power required to validate transactions and mine blocks on a proof-of-work blockchain.

Difficulty Bomb

The process of making a proof-of-work blockchain more difficult to use in order to encourage users to switch to a different consensus method (such as proof-of-stake in the case of Ethereum).

DYOR stands for "Do Your Own Research."

This term, like DD, is used to urge consumers to do their own research about an asset before investing in it.

Ethereum Improvement Proposal (EIP).

A common framework for submitting a new feature to the Ethereum community.

Ethereum Request for Comments (ERC)

A standard smart contract framework that Ethereum-based smart contracts are built on.

Ethereum

Ethereum is a decentralised application platform built on top of a public blockchain. Ethereum is a turing complete language that allows users to create and deploy sophisticated, self-executing smart contracts on the blockchain.

Fiat

A currency (like US Dollar) introduced as a legal tender and is supported and regulated by a government entity.

FOMO

FOMO stands for "Fear Of Missing Out." A sensation of anxiety coming from the loss of an opportunity. This generally happens when investors acquire an asset after it has already seen a significant price gain, expecting to get in and out before a downturn occurs.

Fork

Changing the protocol of a blockchain is called forking it. It results in a soft fork when the modifications are small. When the modifications are more fundamental, a hard fork may occur, resulting in the development of a second chain with its own set of rules.

Fractionalising

To fractionalize the process of securing an NFT in a smart contract and then breaking it into smaller pieces that are distributed as fungible tokens. This decreases the cost of ownership and enables a community to own artwork and other digital assets.

FUD

Fear, Uncertainty, and Doubt (FUD) news about an asset that seems to be unfavourable but turns out to be erroneous or exaggerated.

Full node

A full node is a blockchain node that records the whole history of the blockchain as well as validates and relays transactions.

Fungible

Interchangeable with anything of a similar kind.

Gas

On the Ethereum blockchain, gas is the cost paid by a user to complete a transaction or execute a smart contract. This cost is determined by the transaction's complexity as well as the network's current demand.

Genesis Block

A blockchain network's very first block is known as the Genesis Block.

Gwei

Gwei is an ether denomination that is used to calculate Ethereum gas pricing. 1 ether = 10⁹ gwei

Hard Fork

A hard fork is a major modification to a blockchain that is incompatible with the present protocol and necessitates the creation of a new chain.

Hashing

Hashing is the process of taking any size input and turning it into a fixed-length fingerprint. Using a unique identifying code, hashing enables a collection of data to be encrypted, saved, and remembered. This is the foundation of blockchain technology, enabling for the safe verification and storage of data and transactions.

Hash rate

The pace at which a computer can create guesses to a cryptographic problem is known as hash rate, or hash power. On a proof-of-work blockchain, the hash rate may also refer to the total amount of power consumed by the whole network.

HODL

A phrase that means "hold" and is commonly interpreted as an abbreviation for "Hold On for Dear Life." This phrase originated as a mistake on the Bitcointalk.org forum, when a member indicated that he was "HODLING" his bitcoin as the price fell. The misspelling became popular quickly and is still in use today.

ICO - Initial Coin Offering

The sale of tokens to the general public in order to generate funds for a crypto-based business is known as an ICO. ICOs are a kind of crowdfunding that is comparable to a typical company's initial public offering (IPO).

IEO - Initial Exchange Offering

An initial exchange offering, like an initial coin offering, or ICO, is a technique of selling tokens to generate funds, but with more regulation. An IEO is operated by an existing cryptocurrency exchange, unlike an ICO, which sells new tokens directly to the public. IEOs aim to make the ICO process more safe by partnering with a well-known and recognised exchange.

Light node

A blockchain node that just downloads enough data from the blockchain to process and validate transactions is known as a Light Node. Light nodes, unlike full or master nodes, do not record the whole history of a blockchain.

Liquidity

The ease with which an item may be purchased, sold, or exchanged in a specific market or on an exchange can be termed as liquidity.

Liquidity Pool

A pool of user-provided money that are locked inside a smart contract to make trading on a DeFi platform easier.

Market Cap

The overall worth of an asset based on its current market price is known as its market cap. The market capitalization of a cryptocurrency is calculated by multiplying the price of a single coin by its circulating supply.

Master Node

A master node is a blockchain node that validates and transmits transactions, records the blockchain's entire history, and may vote, control the network, and perform other specialized roles.

Metaverse

A simulated digital environment that combines augmented reality (AR), virtual reality (VR), blockchain, and social media principles to create areas for rich user interaction that mirror the actual world.

Mining

Mining is the process of confirming transactions, arranging them into blocks, and then adding blocks to the blockchain under a Proof of Work system. Miners are those who participate in this procedure.

Minting

Minting is the process of confirming and certifying info on the blockchain, such as domain ownership.

To the moon

This term suggests that the value of an asset will rise to the point that it will literally reach the moon. This is practised by shills during a bull market.

Moonboy

Moonboy is a nickname used to describe excessively enthusiastic social media "financial gurus" who are continuously emphasizing how a specific asset (mostly cryptocurrencies) is "heading to the moon!"

NFT

A non-fungible token (NFT) is a digital certificate of authenticity that is used to allocate and verify ownership of a single digital or physical item. NFTs are not convertible with each other, unlike fungible tokens.

NFT domains

NFT Domains are blockchain-based domain names that enable users to establish their Web3 username.

NGMI

The acronym NGMI stands for "not going to make it." This term is used to indicate that a project or asset has a low likelihood of becoming valued. This may also be aimed against a specific person, notably someone who has made a disastrous investment or transaction.

No-coiner

No-coiner is a word used to describe someone who does not own any cryptocurrencies or is inexperienced with cryptocurrency in general.

Node

Any device that is linked to a blockchain network is referred to as a node. Different nodes have different degrees of responsibility and may be used to verify transactions, maintain the blockchain's history, transmit data, and perform other tasks. Nodes join together to construct the network's architecture since blockchains are dispersed peer-to-peer networks.

Oracle

Oracle is a service that provides data from the outside world to smart contracts. Because smart contracts can't access data outside the blockchain, they depend on oracles to retrieve, validate, and deliver external data.

P2P

A dispersed network of two or more computers that connect directly without the need of a central server or organisation.

Private Key

A private key is an alphanumeric passcode that may be used to withdraw funds from a blockchain wallet and to approve digital transactions. Because these private keys are lengthy and difficult to recall, wallets usually pair them with a recovery phrase.

Proof of stake

Proof of Stake (PoS) is a consensus process in which validators, or nodes, stake a certain amount of bitcoin on the blockchain in order to validate transactions and mint blocks. If a validator confirms a fraudulent transaction, they will lose a piece of their investment.

Proof of work

Proof of Work (PoW) is a consensus process in which miners are required to solve challenging mathematical problems in order to validate transactions and mint blocks. When a miner solves a challenge properly, they acquire permission to mint the next block and collect the block reward.

Public Key

This is an alphanumeric code that acts as the address for a blockchain wallet, comparable to a bank account number.

Pump and dump

A pump-and-dump strategy is one in which a cryptocurrency or other asset is pumped up, causing many people to acquire it and drive up its price. Those that hyped the asset then sell their interests when the price increases for a brief period of time. This causes a quick selloff, with everybody who did not sell losing money.

Rug Pull

Rug pulls a scam when a crypto enterprise takes the cash entrusted in its system and runs with them. Rug pulls may also happen in assets with a centralised ownership structure.

Rollup

Rollup is a scaling technique that tries to increase transaction throughput while lowering costs by batching several transactions off-chain and then sending them as a single transaction to the main chain.

Satoshi

Satoshi is the lowest unit of Bitcoin, equaling 0.00000001 bitcoin.

Seed Phrase

A seed phrase is a set of words that is used as a master password to access a cryptocurrency wallet. Because a single wallet may hold numerous accounts, each with its own private key, a seed phrase makes it simple to log in to all of them using the same password.

SHA-256

The Secure Hashing Algorithm (SHA) is a collection of cryptographic hashing algorithms developed by the National Security Agency (NSA). SHA-256 takes an input of data and creates a hash, which is a lengthy series of letters and numbers. This hash is then used to represent the data in a safe manner.

Sharding

Sharding is a technique for breaking down a network's nodes into smaller groups (shards) in order to improve scalability. These shards may then achieve a consensus on behalf of the whole network, eliminating the requirement for each node to execute each transaction.

Shill

The practice of extensively advertising a cryptocurrency, stock, or other asset in order to boost acceptance and, as a result, enhance its price. This is mainly accomplished via social media spamming.

Shitcoin

Shitcoin is a cryptocurrency with questionable foundations and little to no practical use.

Sidechain

A sidechain is a separate blockchain that is used to unload transactions off the main chain in order to improve scalability or add new features.

Slippage

Between the moment an order is made and the time it is filled, the price of a cryptocurrency may vary. The gap between a cryptocurrency's advertised price and the price at which a deal actually executes is referred to as slippage.

Smart Contract

On a blockchain, a smart contract is a self-executing code. Smart contracts eliminate the need for an intermediary and eliminate the need for the parties involved to trust one another.

Soft Fork

A soft fork is a blockchain upgrade that is backwards compatible. These modifications do not need the formation of a new chain, unlike a hard fork.

Solidity

Ethereum's native programming language, Solidity, is primarily used to create smart contracts.

Stablecoin

A stablecoin is a token whose value is linked to the value of another asset. Stablecoins are normally backed by a fiat currency, such as the US dollar, but they may also be backed by tangible assets such as precious metals.

Testnet

The testnet is a software environment that simulates the mainnet blockchain and is used to test network updates and smart contracts before they are deployed to the mainnet.

TLD

The final component of a domain name, or the portion that comes after the "dot" sign, is known as the TLD. (Ex: .nft, .eth, etc.)

Token

Tokens are used to represent digital and physical assets, as well as to interact with decentralised applications (dapps).

TPS

TPS stands for Transactions Per Second, which is the amount of transactions a blockchain can process per second and is used to gauge its computing capability.

Total Value Locked

Total Value Locked (TVL) is a measurement of the assets locked within a smart contract for a dapp, commonly represented in USD.

WAGMI

"We're All Gonna Make It," a popular phrase in crypto and trading circles that denotes friendship and optimism.

Wallet

The private keys of blockchain assets and accounts are stored in a wallet, which can be a software program or a hardware device. A blockchain wallet, unlike a typical wallet, does not store the currencies or tokens itself. Instead, they save the private key that certifies a digital asset's ownership.

Wallet Address

Wallet Address, also known as a public key, is an alphanumeric code that acts as a wallet's address, comparable to a bank account number.

Web1

Web1 is the earliest version of the internet, sometimes known as the "read-only web." Web1 was defined by information-based static webpages. User involvement and user-generated material were minimal.

Web2

The "read-write web," which began in the 1990s, is distinguished by user-generated content and enhanced user interfaces. As a result, blogs and social media platforms were born. Web2 put a greater focus on user experience and interoperability across various apps and websites, resulting in the large network of linked websites and services we are acquainted with today.

Web3

Web3 is the next generation of the internet, which will make use of blockchain technology, open-source apps, and data and information decentralisation. Web3 aspires to take control of the web away from monopolistic tech giants and give people back control of their data and content. The "read-write-trust web" is another name for it.

Wei

Wei is the lowest ether denomination, named after Wei Dai, a cypherpunk and cryptocurrency pioneer. 1 ether = 10^{18} gwei

51% attack

An assault in which one entity or group gets control of more than 50% of a network's nodes or mining power. This enables the organisation to cause network disruption by blocking particular transactions, double-spending crypto, and engaging in other malicious behaviour.