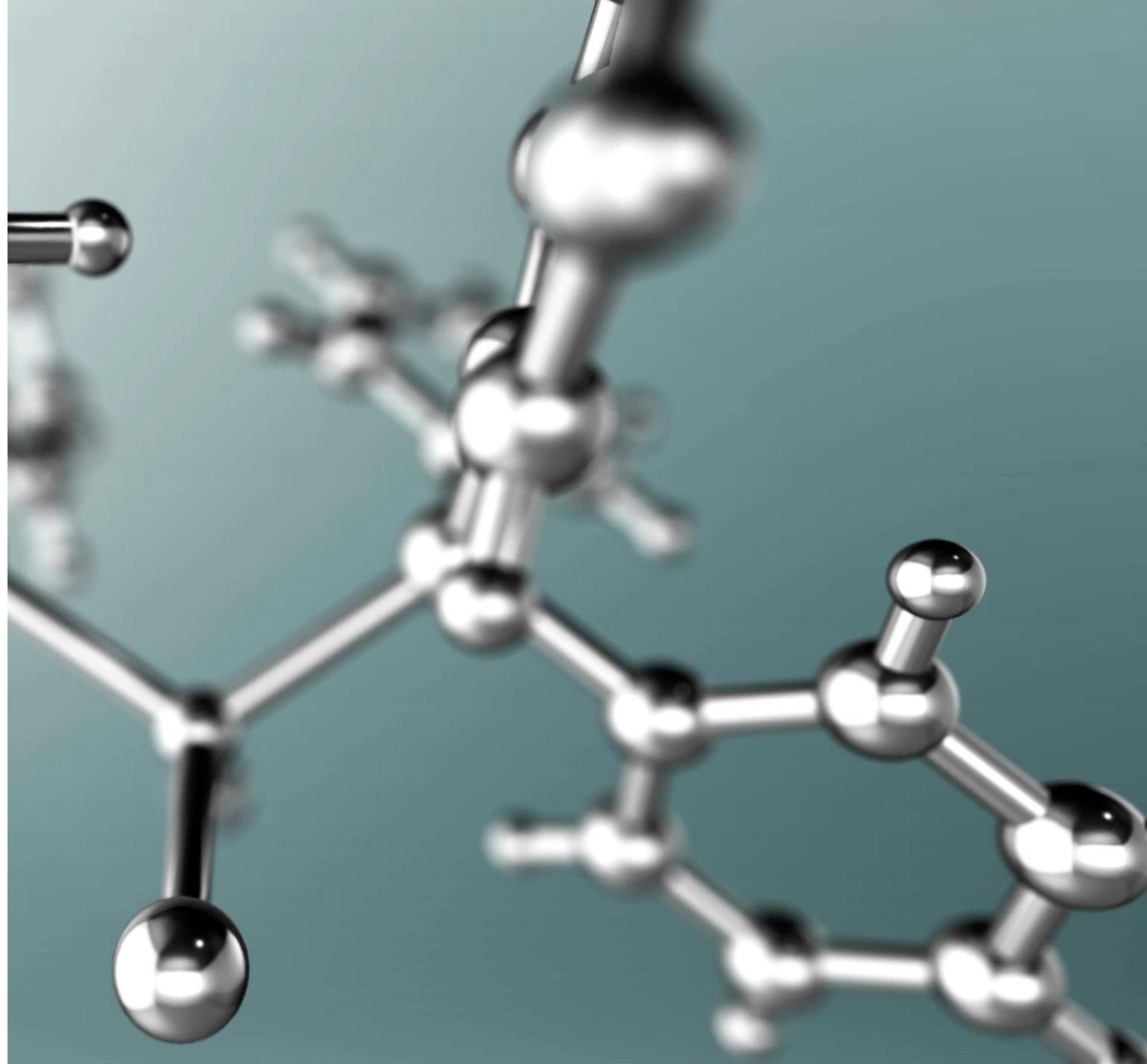

Blockchain Applications

30.01.2022

Bhagirath Kumar Lader
Chief Manager (BIS)
GAIL (India) Limited

ai79bh@gmail.com

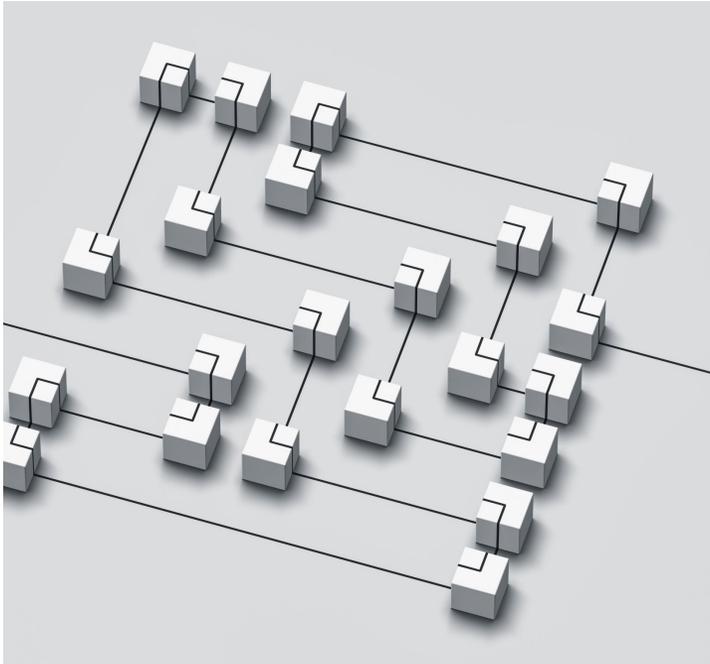


Agenda

- What is Blockchain Technology
- Features of a Blockchain System
- Blockchain Ecosystem
- Blockchain Applications
 - What is the meaning of an (crypto) asset
 - How blockchain can be used as a trusted
 - What are decentralized apps
 - Token Economy
 - Crypto World and NFTs
 - Other Blockchain Applications



What is Blockchain



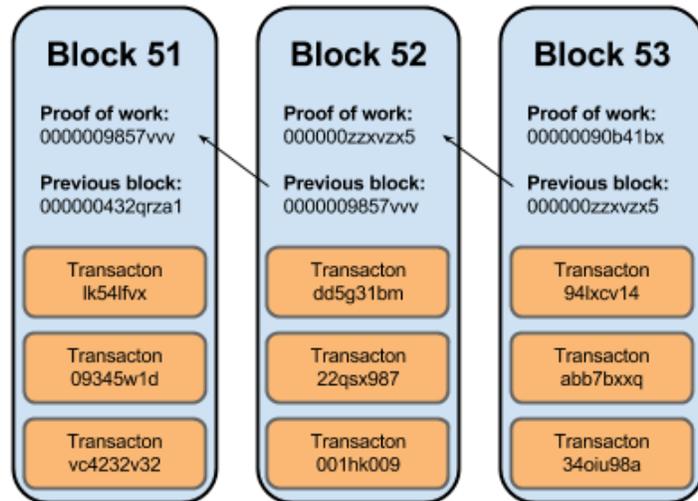
- **Blockchain** is a technology that allows for a **distributed ledger** that keeps track of all changes, or transactions that occur within a network. This ledger is **decentralized** and is hosted on every system that is a part of it (members of the system are known as **nodes** or **peers**), rather than one isolated server.
-

Blockchain – a Revolutionary technology for the future



- A Blockchain is a (digital) diary that is almost impossible to forge. Blockchain technology is disrupting and transforming the Business of Trust.
- All the data stored on a blockchain is recorded digitally and has a common history which is available for all the network participants. This way, the chances of any fraudulent activity or duplication of transactions is eliminated without the need of a third-party.
- Each transaction on a blockchain is secured with a digital signature that proves its authenticity. Due to the use of encryption and digital signatures, the data stored on the blockchain is tamper-proof and cannot be changed.
- Each block in a blockchain network stores some information along with the hash of its previous block. A hash is a unique mathematical code which belongs to a specific block. If the information inside the block is modified, the hash of the block will be subject to modification too. The connection of blocks through unique hash keys is what makes blockchain secure.

Blockchain – A Business Definition

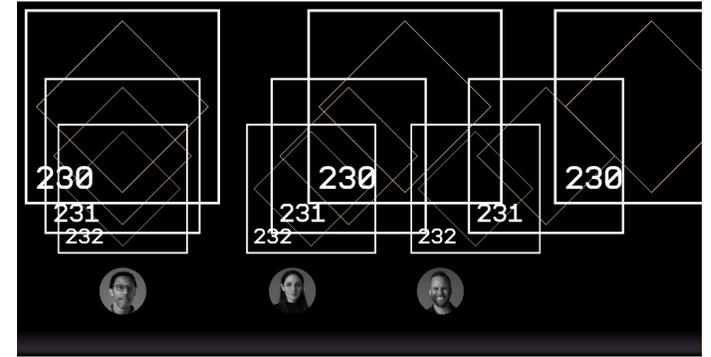


- Blockchain may be defined as a technology platform whereby peers (participant computers) can exchange values (digital assets) using transactions without the need for a centralized trusted arbitrator (like a central server or bank or RBI or regulatory agency).
- Blockchain is peer-to-peer, append-only shared or distributed datastore (like a ledger or diary or spreadsheet) that uses consensus to synchronize cryptographically-secured data.
- Blockchain is simply a selection of transactions bundled together in order to organize them logically. A reference to previous block is also included in the block unless it is the genesis or first block in the blockchain.

Blockchain – A Technology of Trust

Establishing Trust

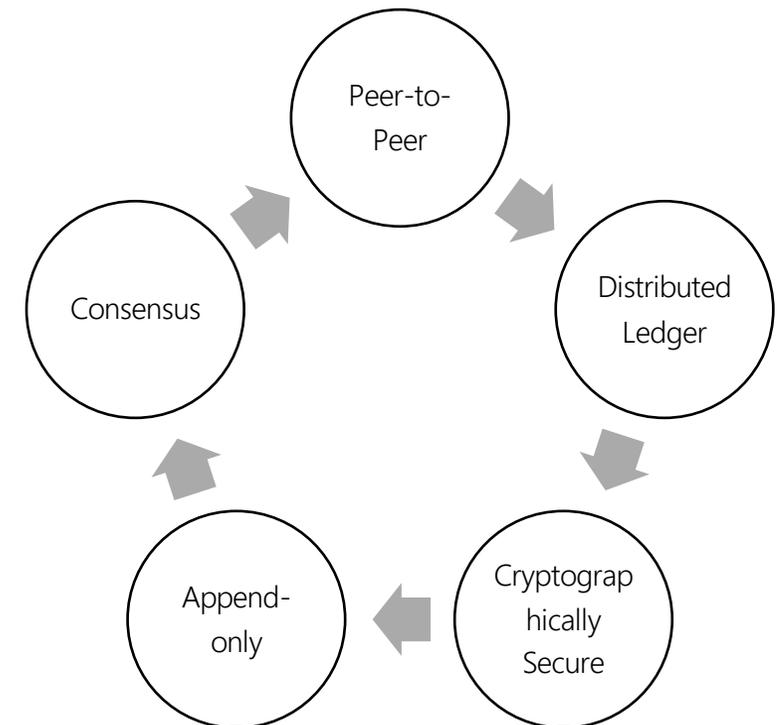
- Each block is stamped with a unique cryptographic code, ensuring records cannot be counterfeited or changed.
- Since all participants have a copy of the entire blockchain, they can detect any tampering.
- So when the hashes match up across the chain, all parties know that they can trust their records.



Revisiting Blockchain definition

Layman's definition: Blockchain is an ever-growing, secure, shared record keeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update.

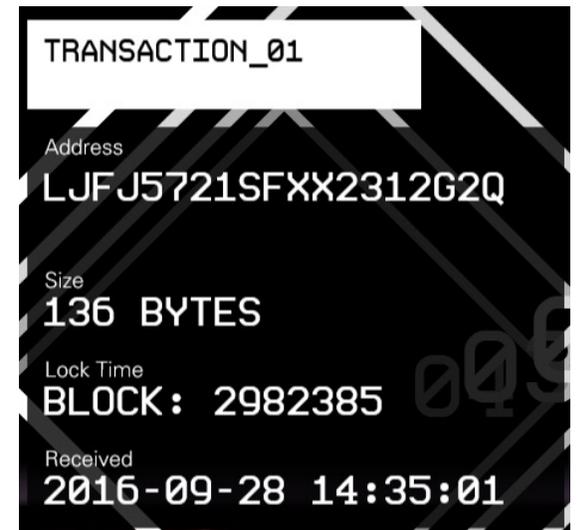
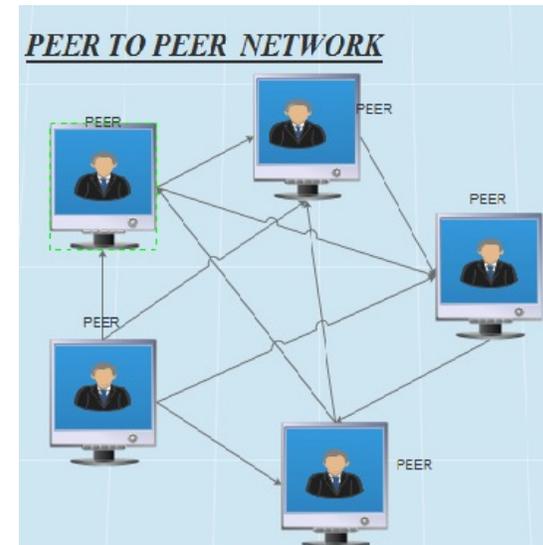
Technical definition: Blockchain is a peer-to-peer, distributed ledger that is cryptographically-secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.



The first blockchain was conceptualized by a person (or group of people) known as [Satoshi Nakamoto](#) in 2008. It was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public [ledger](#) for all transactions on the network.

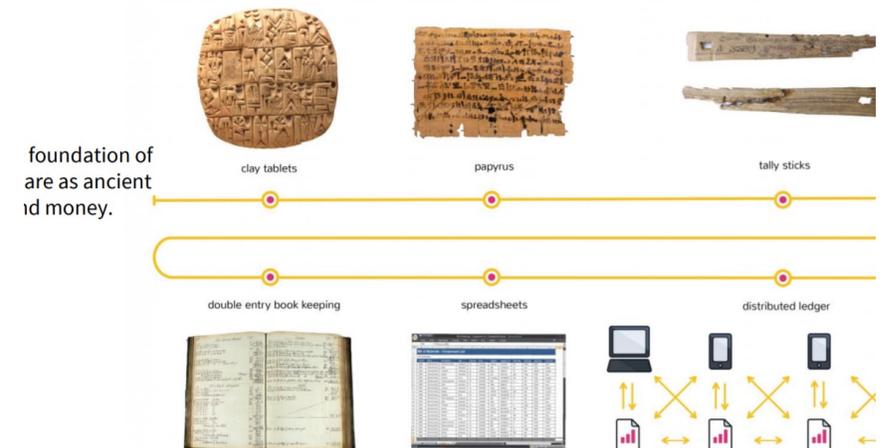
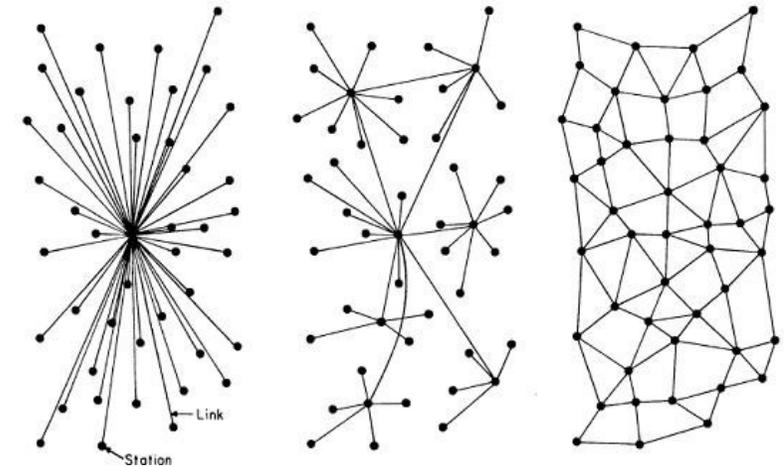
Peer-to-peer

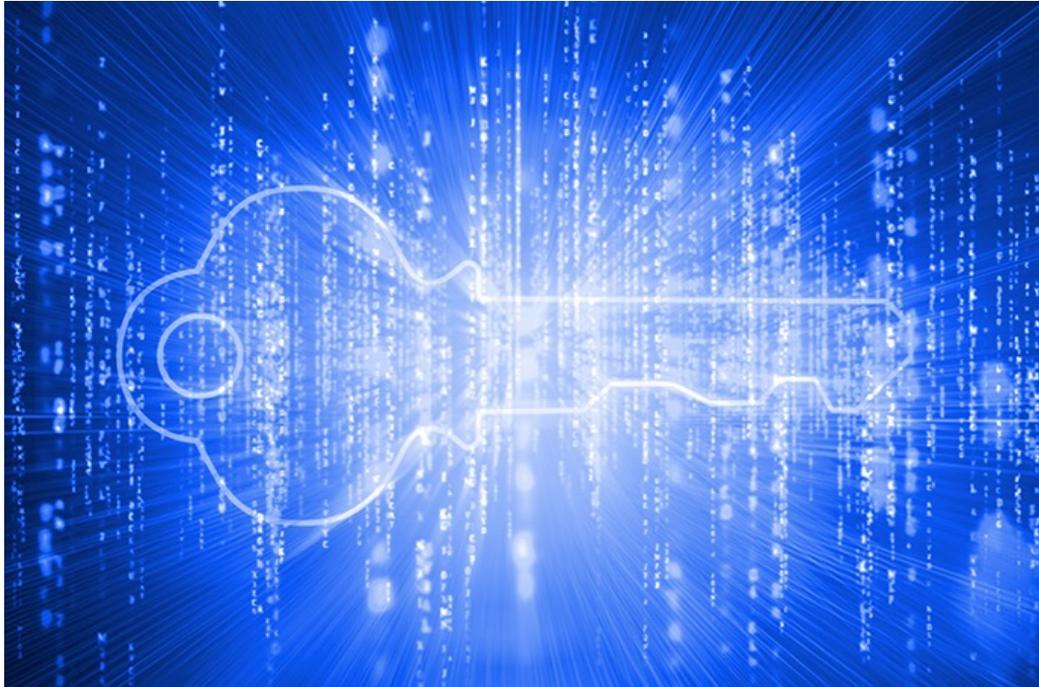
- There is no central controller in the network
- All participants talk to each other directly
- This property allows for cash transactions to be exchanged directly among the peers without a third-party involvement, such as by a bank.



A Distributed Ledger

- Blockchain is a distributed ledger which means that a ledger is spread across the network among all participants (peers or computers) in the network
- Each peer holds a copy of the complete ledger





Cryptographically secure

- Cryptography has been used to provide security services which make this ledger secure against tampering and misuse
- These services include non-repudiation, data integrity, and data origin authentication.
- **Confidentiality** is the assurance that information is only available to authorized entities.
- **Integrity** is the assurance that information is modifiable only by authorized entities.
- **Authentication** provides assurance about the identity of an entity or the validity of a message.

Cryptographically secure

```
t3mbozW+E7zdWkrYIi1TGV70v03EUpmWFIig0VBpAw3
be1bQD0BWU447j5PfuPBoF7eCfyqyKg/gDh/ncfku2Y
4pE55FgaLqb0ujTrvHUX0PqCG2GnwCERj21axeom0F
cte0zspo0z0kYqoMwTubtnmzcsspjtYwXK6+RyoC4AD
0ngwLHNBAcRtLrzmlDEaAJrbfQm8tZpu8rP6EYv3kNe
RE3+cVaFr8HspvpM8SxMb0vYtZ2XJ6j7x2eB2PFDjkd
6nkctkAV1UtFwbpZIm0xkIi6XwhY2apeGxp24r0AaKa
8kygM0nRn5jSdt6/XeNcAScxaeEKedUTv0vSSlHIZJS
9lBxIFU2jzKrv3hKnMGoVaXGoh2XJMedjPM0gLupRbP
0aTQkX6d9GxnWwe4mfVKSbxg68rsueGn4x98oZ00Tb7
8PZpmlqjcfxoXGEjARDp4NP7gESaXXjw4Juvbgg7FnZ
LPG43fdvZ6KBQYQjPTgiheB5auLaKny03i9DlxckKXZ
xkAtnxHvNeyduoics10f/9tvAehunJA0lgp1IvdD47Z
YbAhcwq+CQdyg5nc1D6ufI0JnXSzNoqznSVWiIiNysm
PmMR5QiK7a1bdYzdrat0wYGB0439fkSr/UmEJyNVQUv
MhTx4STSkUc0xQu2zTmfrk2abmXzNcAJEnpQrtysJ0
tJ0HYbdWraApdpPxVItxTA7A6sLWbn3kttjaitKlCuW
HBC61poFtBTqaIoewbKxHyJ76ZvQeNzZNdG3d/5I9EC
8z9qvML/57tlRaxFqwLdfbAmrUFyh0wzvC2jS9IEoQe
tR2vJFwQx9CyDjNfxIK0cC7pGzZtW9TVX7AG93QTTo0
/V38EK/Gap+kc39J87QzrhBUcWooQjgbZ8aZtx9b/89
+SPR+KReniJM7A6e0n6fK0UJQ0T2qp832J5ilQ7FzTR
/t9BBQKQuL2tX6CxyXzZ20aRwK+DC0RkWIgfocdPeWC
48dd3mpPmn5Lf3NEUALzSwLM0ct0sZ0Y3bV4ez+hXzf
tUYhbNSrtS39gC0THiVNdqHnmcc+IDAG7JHrFXvNvLX
```

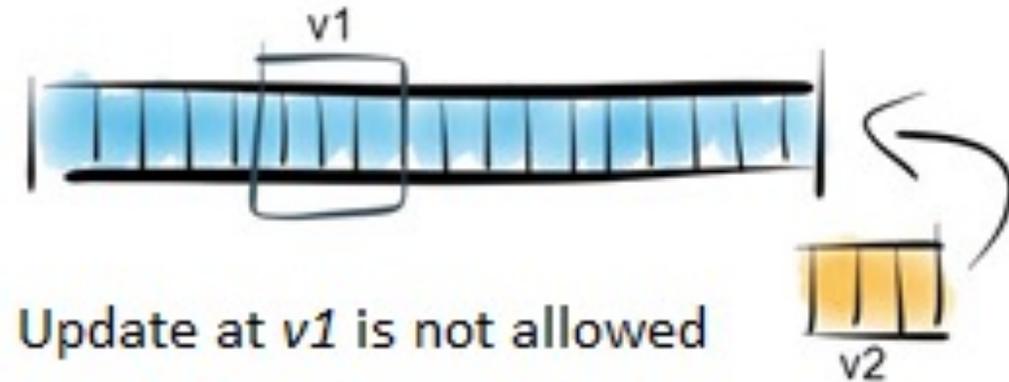
- Data origin authentication, also known as *message authentication*, is an assurance that the source of the information is indeed verified.
- Non-repudiation is the assurance that an entity cannot deny a previous commitment or action by providing incontrovertible evidence. It is a security service that offers definitive proof that a particular activity has occurred. This property is essential in debatable situations whereby an entity has denied the actions performed, for example, placement of an order on an e-commerce system. This service produces cryptographic evidence in electronic transactions so that in case of disputes, it can be used as a confirmation of an action.
- **Hash functions** are used to create fixed-length digests of arbitrarily-long input strings. Hash functions are keyless, and they provide the data integrity service. They are usually built using iterated and dedicated hash function construction techniques.

How Blockchain keeps blocks safe from tampering

- Each block in a blockchain is connected to all the blocks before and after it. This makes it difficult to tamper with a single record because a hacker would need to change the block containing that record as well as those linked to it to avoid detection. A blockchain has some other inherent characteristics that provide additional means of security.
- The records on a blockchain are secured through cryptography. Network participants have their own private keys that are assigned to the transactions they make and act as a personal digital signature. If a record is altered, the signature will become invalid and the peer network will know right away that something has happened. Early notification is crucial to preventing further damage.
- Blockchains are decentralized and distributed across peer-to-peer networks that are continually updated and kept in sync. Because they aren't contained in a central location, blockchains don't have a single point of failure and cannot be changed from a single computer. It would require massive amounts of computing power to access every instance (or at least a 51% majority) of a certain blockchain and alter them all at the same time.



Append-only



- *append-only property* means that data can only be added to the blockchain in *time-ordered sequential order*
- This property implies that once data is added to the blockchain, it is almost impossible to change that data and can be considered practically immutable.
- Nonetheless, it can be changed in rare scenarios wherein collusion against the blockchain network succeeds in gaining more than 51 percent of the power.
- For all practical purposes, blockchain is indeed immutable and cannot be changed.

Consensus based update



- For any update, Blockchain technology allows all the network participants to reach an agreement, commonly known as consensus.
- This is what gives it the power of decentralization. In this scenario, no central authority is in control of updating the ledger.
- Instead, any update made to the blockchain is validated against strict criteria defined by the blockchain protocol and added to the blockchain only after a consensus has been reached among all participating peers/nodes on the network.
- To achieve consensus, there are various consensus facilitation algorithms which ensure that all parties are in agreement about the final state of the data on the blockchain network and resolutely agree upon it to be true.

Smart Contracts



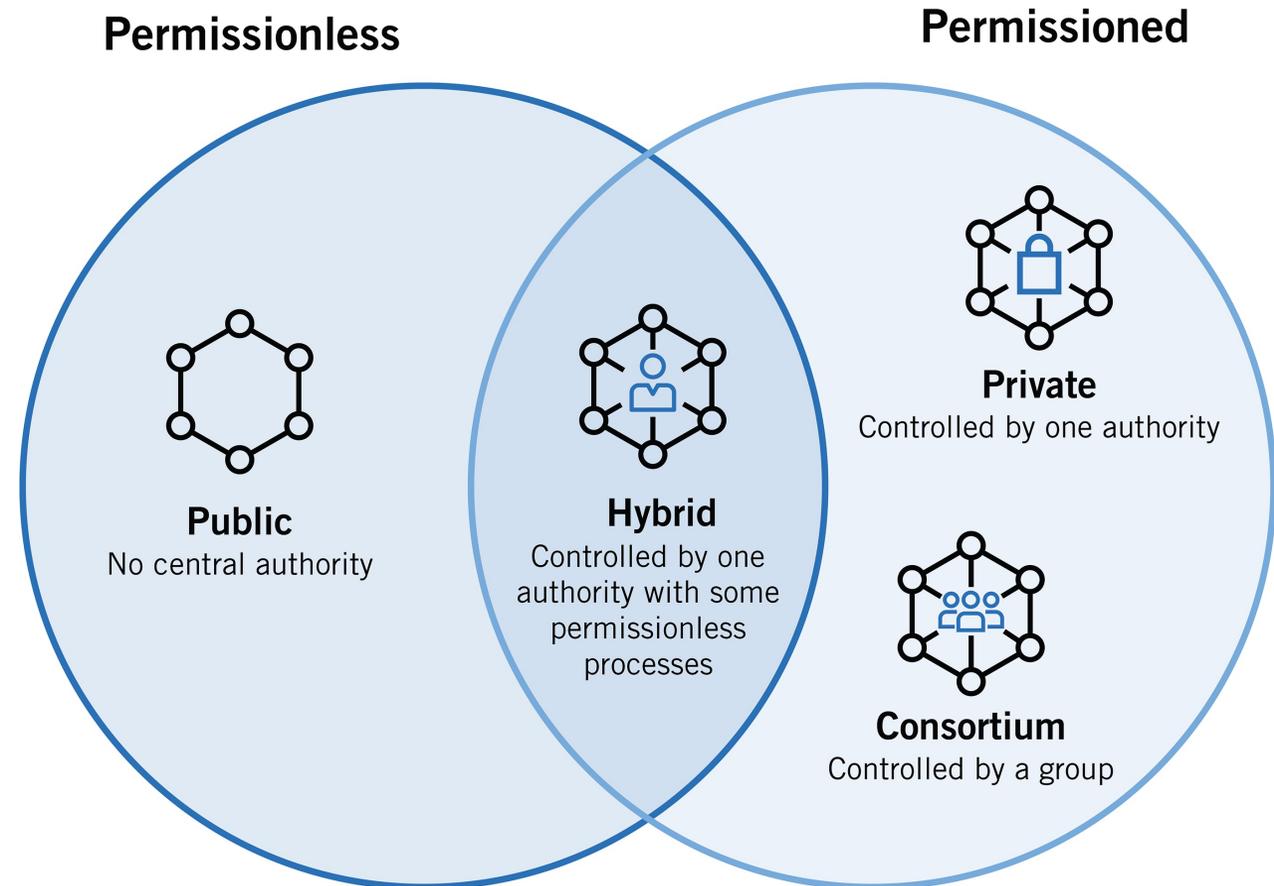
- Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met.
- They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss.

A glowing green padlock is centered on a blue circuit board background. The padlock is illuminated with a bright green light, making it stand out against the darker blue background. The circuit board has various traces and components visible, creating a complex, technical appearance. The overall color palette is dominated by blues and greens, with the green of the padlock being the most vibrant element.

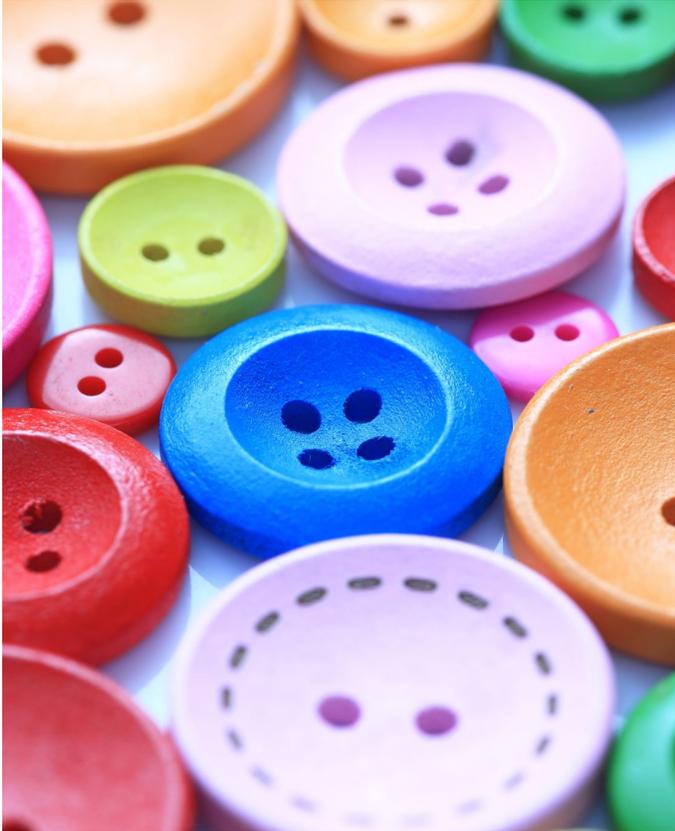
BLOCKCHAIN ECOSYSTEM

Types of Blockchains

- Permissioned Blockchains
- Permissionless Blockchain



Types of Blockchains

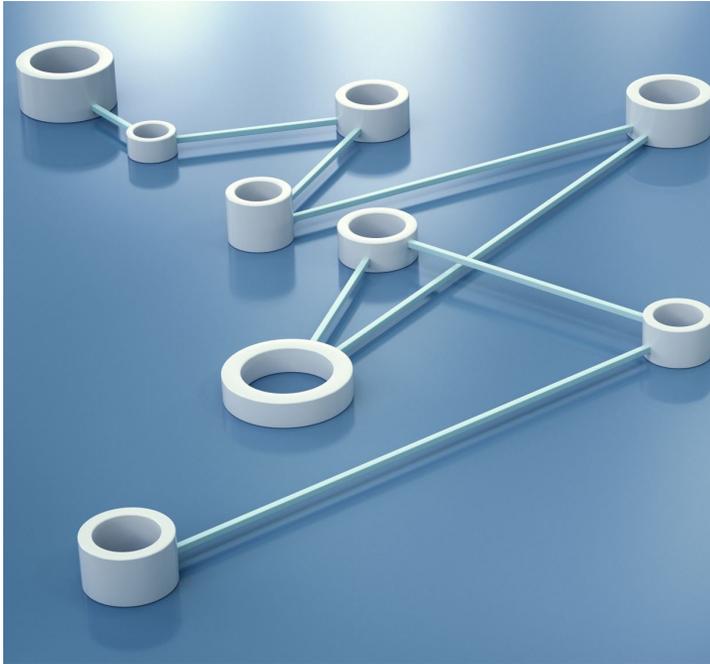


- **Public blockchains** are permissionless in nature, allow anyone to join, and are completely decentralized. Bitcoin and Ethereum.
- In a **Private blockchain**, the central authority determines who can be a node. The central authority also does not necessarily grant each node with equal rights to perform functions. Ripple and Hyperledger.
- **Consortium blockchains** are permissioned blockchains governed by a group of organizations, rather than one entity, as in the case of the private blockchain. R3 and CargoSmart.
- **Hybrid blockchains** are blockchains that are controlled by a single organization, but with a level of oversight performed by the public blockchain, which is required to perform certain transaction validations. IBM Food Trust.

Leading Blockchain Platforms

- Ethereum (2013)
 - IBM Blockchain
 - Hyperledger Fabric
 - Hyperledger Sawtooth
 - R3 Corda
 - Tezos (2014)
 - EOSIO (2018)
 - Steller
 - Quorum
 - Ripple
 - Tron
 - Multichain
 - Open-chain
 - NEO
 - Microsoft Azure Blockchain
 - Oracle Blockchain Cloud
 - Flow
 - Binance Smart Chain
 - WAX - Worldwide Asset eXchange
 - Tangle by IOTA (future)
-

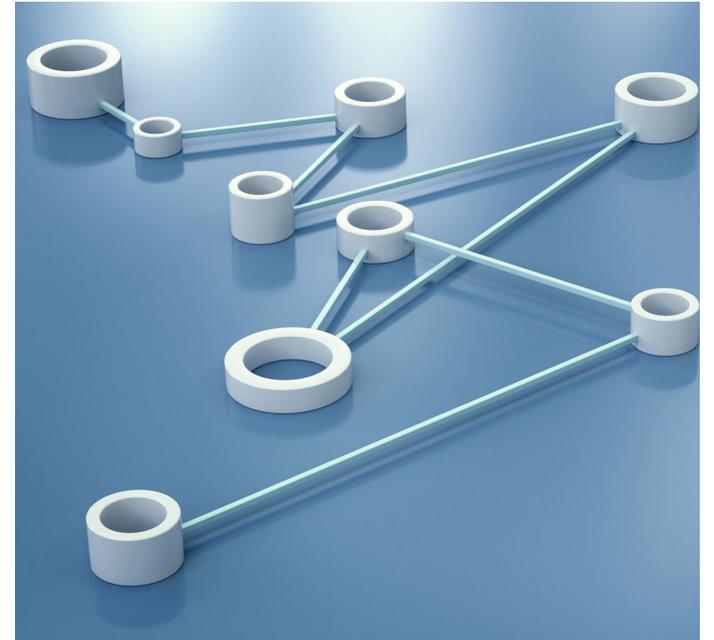
Difference Between a Blockchain Powered DApp and a Simple App



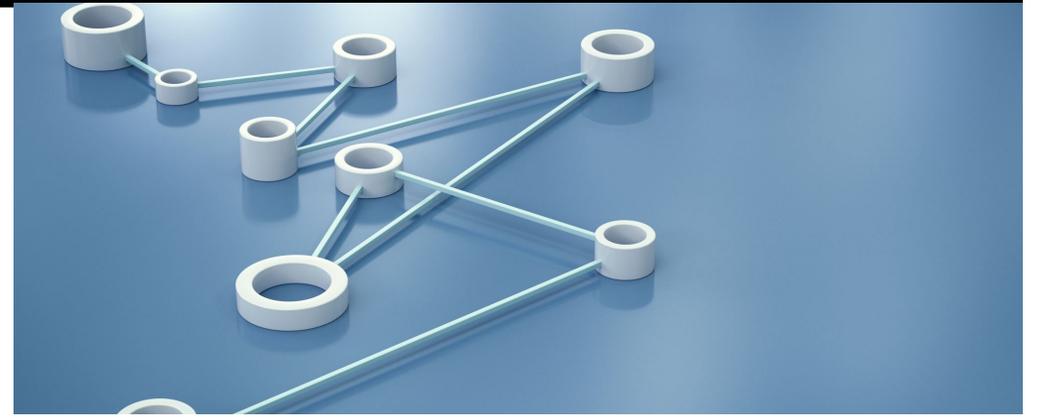
- A DApp, or decentralized app, has its open-sourced backend code running on a decentralized network (P2P network), which offers great features such as transparency, fairness, proof of ownership, etc.
- As many IT technologies have underlying (infrastructure) and application layers, dapp is the application layer for blockchains.

Difference Between a Blockchain Powered DApp and a Simple App (2)

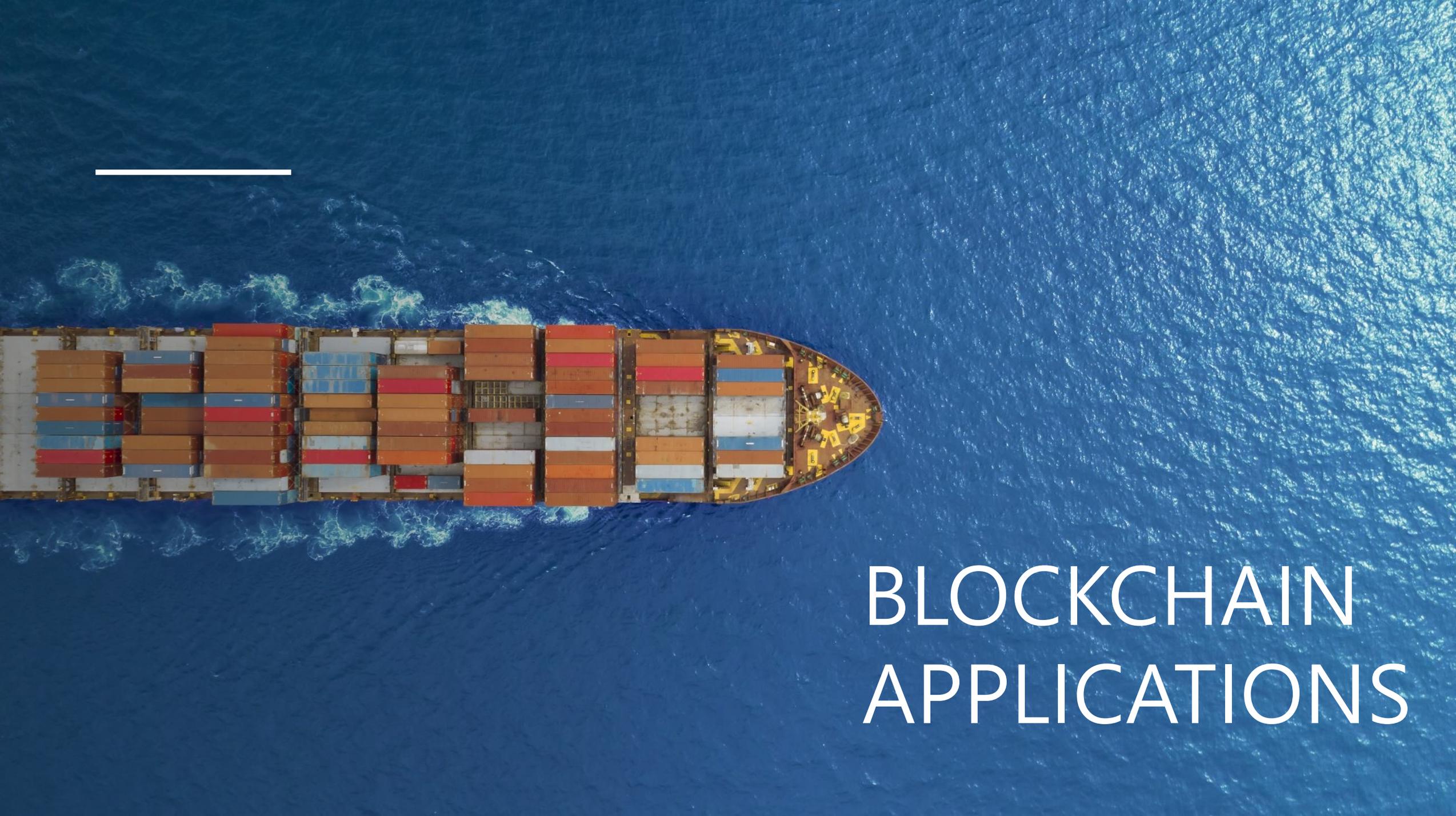
- First of all, a dapp's operation is completely transparent and recorded on the public ledger.
- In addition, its data and transaction cannot be erased once it is generated.
- The key advantages are that a dapp is more trusted by the users, and the users get the control and ownership of their data and assets.



Difference Between a Blockchain Powered DApp and a Simple App (3)



- The current disadvantage is that dapps are not as user-friendly as traditional apps - it still has some limitation due to the scalability of blockchains and it also required more learning process for the users to understand wallets, tokens, transactions etc.
- The dapp industry is still very small when we look at two key figures from our 2018 Dapp Market Report - 1,423 active dapps and 3% usage (1,799,918 dapp users from 54,814,617 accounts) on Ethereum, EOS, Steem, and Tron blockchain. We could easily compare with a number of more than 65,000 apps launched in Apple App Store in its first year.



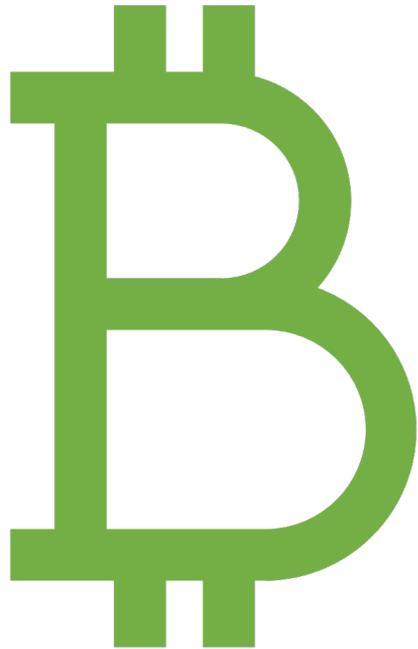
BLOCKCHAIN APPLICATIONS

Asset



- An asset is a resource owned by the business which can be tangible or intangible.
 - Tangible assets are real and measurable, they are physical such as inventory. Intangible assets are digital (not physical). They range from bonds, stocks & digital currencies to intellectual property (trademarks, copyrights, etc.). Trade secrets, training material and licenses are also intangible assets.
-

Tokenization



- Tokenization can be used to represent commodities, real estate, ownership of artwork, currency, or anything else of value as a digital asset on a blockchain.
 - A token can be fungible or non-fungible
-

Tokenization and Token Economy

- A token is a (cryptographic) representation of an object
- A token often represents something that is of a value e.g. a gift voucher that can be redeemed.
- In computing, we use both hardware and software tokens e.g. a hardware security token or a network access token.
- In cybersecurity, we use tokens to substitute a sensitive data with a non-sensitive equivalent e.g. zoom password encrypted through a token on a zoom link.
- In blockchain world, tokens exist digitally on a blockchain and are operated cryptographically i.e. generated, protected and transferred using cryptographic protocols.
- Tokenization converts an asset to a digital token on blockchain



Tokenization and Token Economy



- Cryptoassets are digital assets which use cryptographic techniques to generate a medium of exchange of financial transactions. Cryptocurrencies, utility coins, security tokens are all different types of cryptoassets.
- Money in metaverse or web3 will likely be a cryptocurrency.
- When it comes to the NFT space or NFT world, crypto collectibles or digital collectibles can represent various items including art-works, photographs, images, audio or music files, plain text files (documents, PDFs, or tweets, manuals), 3D models, online game items, virtual properties, virtual worlds, metaverses, web domain names, and other valuable assets.

Blockchain Applications - NFTs



- An NFT is a unit of data stored on a digital ledger, called a blockchain, which can be sold and traded. The NFT can be associated with a particular digital or physical asset (such as a file or a physical object) and a license to use the asset for a specified purpose.
- NFTs, or non-fungible tokens, are unique files that live on a blockchain and are able to verify ownership of a work of digital art. Buyers typically get limited rights to display the digital artwork they represent, but in many ways, they're just buying bragging rights and an asset they may be able to resell later. The technology has absolutely exploded over the past few weeks — and Winkelmann, more than anyone else, has been at the forefront of its rapid rise.



Luxury NFTs

- Luxury NFTs could become a \$56 billion market by 2030 and could see 'dramatically' increased demand thanks to the metaverse, Morgan Stanley says
- Luxury Sees Billions in Rolex, Hermes and Gucci NFTs

Blockchain Applications - NFTs

- NFTs function like cryptographic tokens, but, unlike cryptocurrencies such as Bitcoin or Ethereum, NFTs are not mutually interchangeable, hence not fungible. In economics, fungibility is the property of a good or a commodity whose individual units are essentially interchangeable and each of whose parts is indistinguishable from another part.
- NFTs have been used as a means of exchanging digital tokens that link to a digital file.

The BeyondLife.club marketplace is live now! Fund your wallet and buy your favorite NFTs!

BeyondLife.club | Powered by GuardianLink

Sign In Sign Up Marketplace Drops

BeyondLife.club's Exclusive Marketplace

Did you miss your chance to collect Amitabh Bachchan & Stan Lee's Chakra the Invincible NFTs? We've got you covered! Now get them on the BeyondLife.club Marketplace to bid, buy, and trade.

Access the Marketplace →

Blockchain Applications - NFTs

- While all bitcoins are equal, each NFT may represent a different underlying asset and thus may have a different value.
 - “Everydays,” Winkelmann creates and publishes a new digital artwork *every day*. The project is now in its 14th year. The piece that was sold, *Everydays: The First 5000 Days*, is a collage of Winkelmann’s work starting at the beginning of the project, when he was posting somewhat crude sketches. It runs through years of evolving digital shapes and sceneries up through the beginning of this year, when he was posting *extremely crude* political illustrations.
 - NFTs in artwork, video-game, Fashion or Luxury NFT for online video-game cosmetics, Music NFT, Film NFT, internet meme NFT
-

Blockchain Applications - NFTs

- NFTs, or non-fungible tokens, are unique files that live on a blockchain and are able to verify ownership of a work of digital art. Buyers typically get limited rights to display the digital artwork they represent, but in many ways, they're just buying bragging rights and an asset they may be able to resell later. The technology has absolutely exploded over the past few weeks — and Winkelmann, more than anyone else, has been at the forefront of its rapid rise.
 - “Everydays,” Winkelmann creates and publishes a new digital artwork *every day*. The project is now in its 14th year. The piece that was sold, *Everydays: The First 5000 Days*, is a collage of Winkelmann’s work starting at the beginning of the project, when he was posting somewhat crude sketches. It runs through years of evolving digital shapes and sceneries up through the beginning of this year, when he was posting *extremely crude* political illustrations.
-

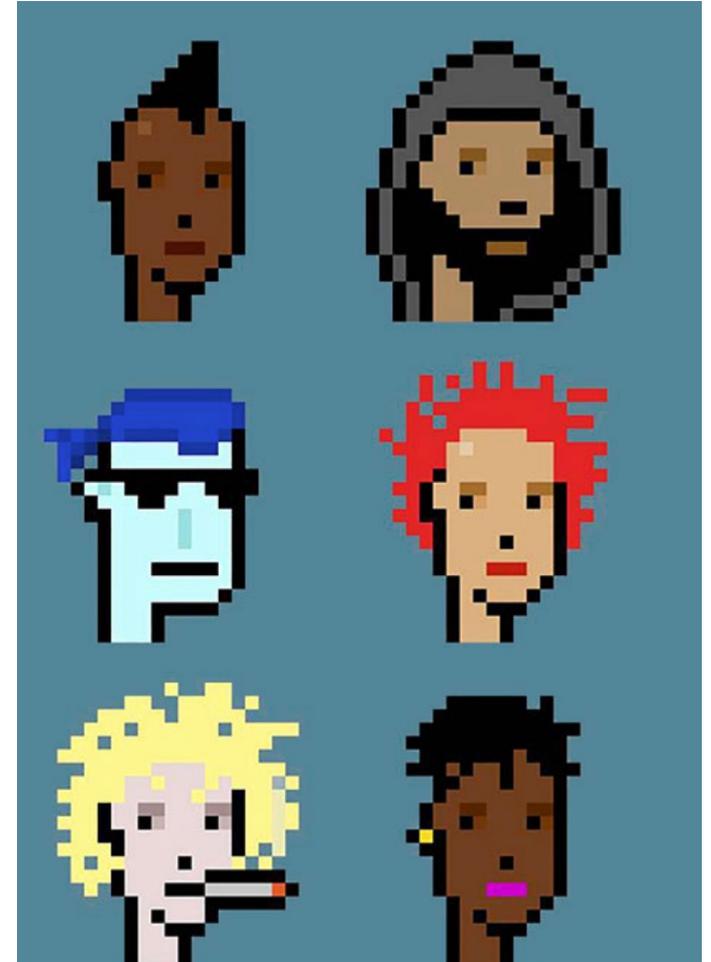


Blockchain Applications – Gaming

- Currently, 60% of the dapps in the market are games.
 - EOS were described as the Las Vegas in blockchain by some media as over 50% of the 60 new dapps launched are betting dapps.
-

NFT Case Study – CryptoPunks

- The CryptoPunks are a collection of 24x24, 8-bit-style pixel art images of misfits and eccentrics. There are exactly 10,000 of them, each with their own ostensible personality and unique combination of distinctive, randomly generated features.
- There are 6,039 male Punks and 3,840 female Punks. A total of 696 wear hot lipstick, while 303 have muttonchops. There are 286 Punks with 3-D glasses, 128 rosy-cheeked Punks, 94 Punks with pigtails, 78 Punks with buck teeth and 44 beanie-wearing Punks.
- There are also eight Punks with no distinctive features at all — sometimes referred to as Genesis Punks — and only one with seven attributes: CryptoPunk 8348 a big bearded, bucktoothed, cigarette-smoking Punk with an earring and a mole, wearing classic shades and a top hat.



NFT Case Study – CryptoPunks

- But only one person can *officially* own a CryptoPunk
 - Official ownership of each work is outlined, in code described by one fan as elegant and [beautifully written](#), in a contract on the publicly accessible Ethereum blockchain. The record, as Larva Labs explained to Christie's, 'is incorruptible and promises to be extraordinarily long-lived.' The ownership history of every artwork is tracked and documented in the blockchain, too.
 - There's a [composite image of all 10,000 CryptoPunks](#) on Larva Labs' website. Anyone can save a copy of the image file to their memory stick or hard drive. Each Punk also has its own page, detailing its special features and complete transaction history.
-

NFT Case Study – CryptoPunks

- The collection of 10,000 Cryptopunks is definitive and unalterable
- In accordance with the nature of blockchain, once the project went live, Larva Labs couldn't alter the existing series, even if they wanted to. 'It's odd to think of what might have been different if we had run the generator just one more time, or used the penultimate run's output.'

The creators regard each work as individual pieces of generative art, while allowing that the entire project itself might be thought of as a larger conceptual piece. 'It's possibly the first work of art with a self-contained mechanism for recording and transacting its ownership.'



NFT Case Study – CryptoPunks

- Once minted, Hall and Watkinson offered the CryptoPunks for free, not forgetting to claim 1,000 for themselves, 'just in case it becomes a thing,' as Hall put it.

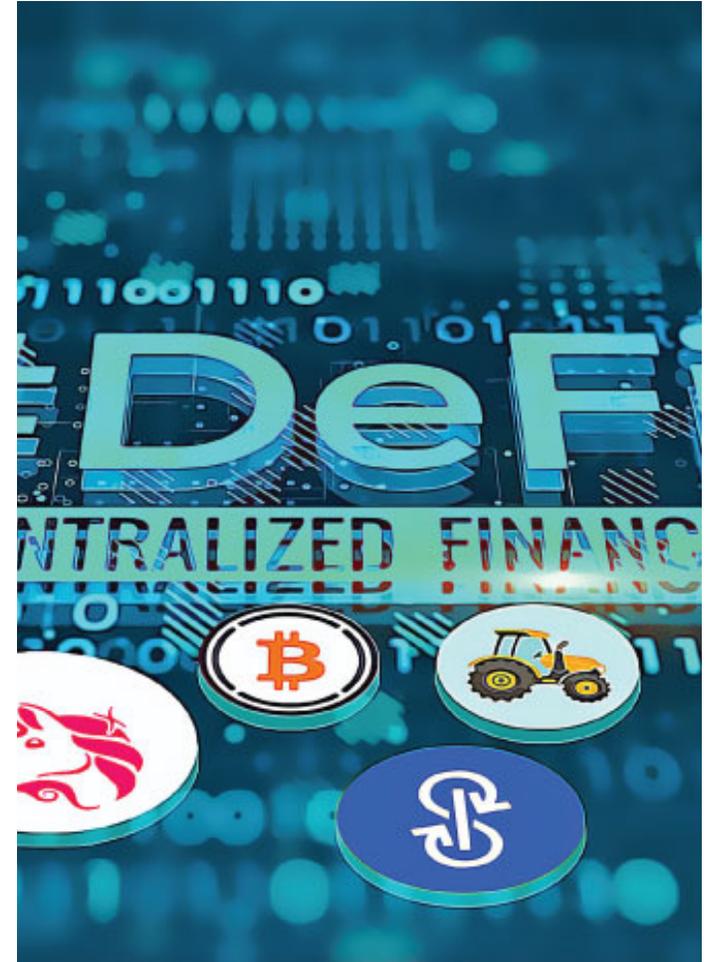
At first, there was very little interest. 'We were starting to think, ah no, this doesn't really have it,' Watkinson has recalled. But before too long, Punks were selling for thousands of dollars.

NFT APPLICATION AREAS



Blockchain Applications – Banking & Financial Markets

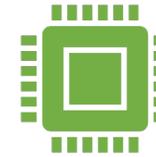
- Decentralized finance (DeFi) is an emerging financial technology based on secure distributed ledgers similar to those used by cryptocurrencies. The system removes the control banks and institutions have on money, financial products, and financial services.
- Some of the key attractions of DeFi for many consumers are:
 - It eliminates the fees that banks and other financial companies charge
 - You hold your money in a secure digital wallet
 - Anyone with an internet connection can use it
 - You can transfer funds in seconds and minutes.



DeFi



Decentralized finance, or DeFi, uses emerging technology to remove third parties in financial transactions.



The components of DeFi are stablecoins, software, and hardware that enables the development of applications.



The infrastructure for DeFi and its regulation are still under development and debate.



Two of DeFi's goals are to reduce transaction times and increase access to financial services.

Blockchain Applications – DeFi

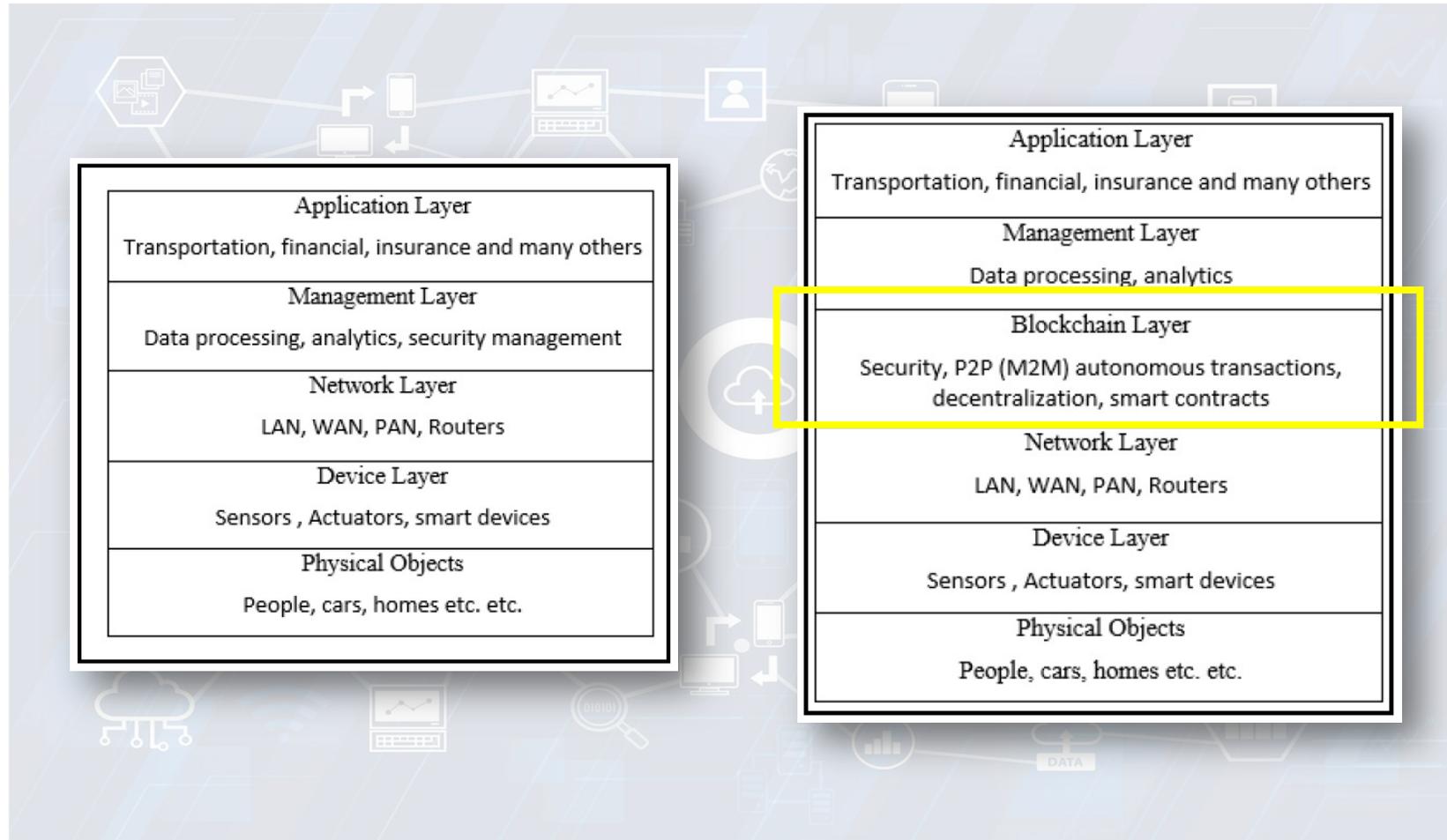
- Various financial instruments – equities, stocks, foreign exchanges, commodities, and various types of derivatives – are traded at these marketplaces.
 - DeFi Dapps are used for lending and borrowing, trading, asset management, insurance, tokenization and prediction markets. Here, trading of tokens on exchanges or decentralized exchanges (DEX) is the prime activity.
 - Regulations are underway to protect the interest of the investors.
-

Blockchain Applications - Government



- Law Enforcement and Border Control – There is a issue of sharing security or intelligence data across various government law-enforcement agencies. Maintaining these information in a smart contract that can be updated as required. Any change will be immediately visible to all agencies.
 - Voting – Blockchain based voting system would provide end-to-end security and transparency. Security means integrity and authenticity of votes. Immutability would guarantee that votes cannot be altered after being casted. It can also prevent double casting of votes. With zero-knowledge-proof, voters can be anonymous.
-

BLOCKCHAIN APPLICATIONS – IOT SECURITY



Blockchain Applications – Healthcare

- Blockchain can be used to decentralize healthcare information, increasing data availability for analytics and research while addressing the issues like data-breaches, high costs, privacy preservation, frauds, etc.
- Issue of counterfeit medicines can be addressed using blockchains, especially in a developing countries like India.
- Blockchain can play significant role in simplifying the process of patient consent, health data exchange and clinical trials management.



Blockchain Applications – Supply Chain

- Increased supply chain transparency
- Build a resilient supply chain using smart contracts
- Streamlined supplier onboarding



Use Cases:

- Vaccine distribution networks
 - Food distribution
 - Container logistics
 - Digital identity verification for procurement
-

Blockchain Applications – Land Registry



- The existing history of transactions on a piece of land first needs to be inserted into the blockchain after approval by Revenue functionaries in the State. The approved data will be digitally signed and stored. This will be a starting point for any mutation.
- The certificates issued by the Revenue Department will be stored in the blockchain and can be used by the other agencies like the bank for any of the verification process during a transaction on the land parcel / farmer.
- Record of Rights document can be accessed by owners and can be verified by agencies requiring it.



Blockchain Applications – Land Registry

Benefits:

- An immutable history of transactional records, so no one can ever doubt the authenticity;
- Records are permanently linked to the system so no one can ever tamper with or forge a record of their own;
- Records can be seen by any party, at any time. It is powerful and validating.

THANK YOU



<https://linkedin.com/in/bhagirathl>

ai79bh@gmail.com