What is a smart contract?

Smart contracts are computer programs that are hosted and executed on a blockchain network. Each smart contract consists of code specifying predetermined conditions that, when met, trigger outcomes. By running on a decentralized blockchain instead of a centralized server, smart contracts allow multiple parties to come to a shared result in an accurate, timely, and tamper-proof manner.
Smart contracts are a powerful infrastructure for automation because they are not controlled by a central administrator and are not vulnerable to single points of attack by malicious entities. When applied to multi-party digital agreements, smart contract applications can reduce counterparty risk, increase efficiency, lower costs, and provide new levels of transparency into processes

How Smart Contracts Work?

Smart contracts are tamper-proof programs on blockchains with the following logic: "if/when x event happens, then execute y action." One smart contract can have multiple different conditions and one application can have multiple different smart contracts to support an interconnected set of processes. There are also multiple smart contract languages for programming, with Ethereum's Solidity being the most popular.
Any developer can create a smart contract and deploy it on a public blockchain for their own purposes, e.g., a personal yield aggregator that automatically shifts their funds to the highest-earning application.
However, many smart contracts involve multiple independent parties that may or may not know one another and don't necessarily trust one another. The smart contract defines exactly how users can interact with it, involving who can interact with the smart contract, at what times, and what inputs result in what outputs. The result is multi-party digital agreements that evolve from today's probabilistic state, where they will probably execute as desired, to a new deterministic state where they are guaranteed to execute according to their code.

Advantages:

Security - Running the contract on blockchain infrastructure ensures there is no central point of failure to attack, no centralized intermediary to bribe, and no mechanism for either party or a central admin to use to tamper with the outcome.

Reliability - Having the contract logic redundantly processed and verified by a decentralized network of nodes provides strong tamper-proof, uptime, and correctness guarantees that the contract will execute on time according to its terms

Equitable - Using a decentralized network to host and enforce the terms of the agreement reduces the ability of a for-profit middleman to use their position of privilege to rent-seek and siphon off value

Efficiency - Automating the backend processes of the agreement--escrow, maintenance, execution, and/or settlement- means neither party has to wait for manual data to be entered, the counterparty to fulfil their obligations, or a middleman to process the transaction

Smart Contract Limitations:

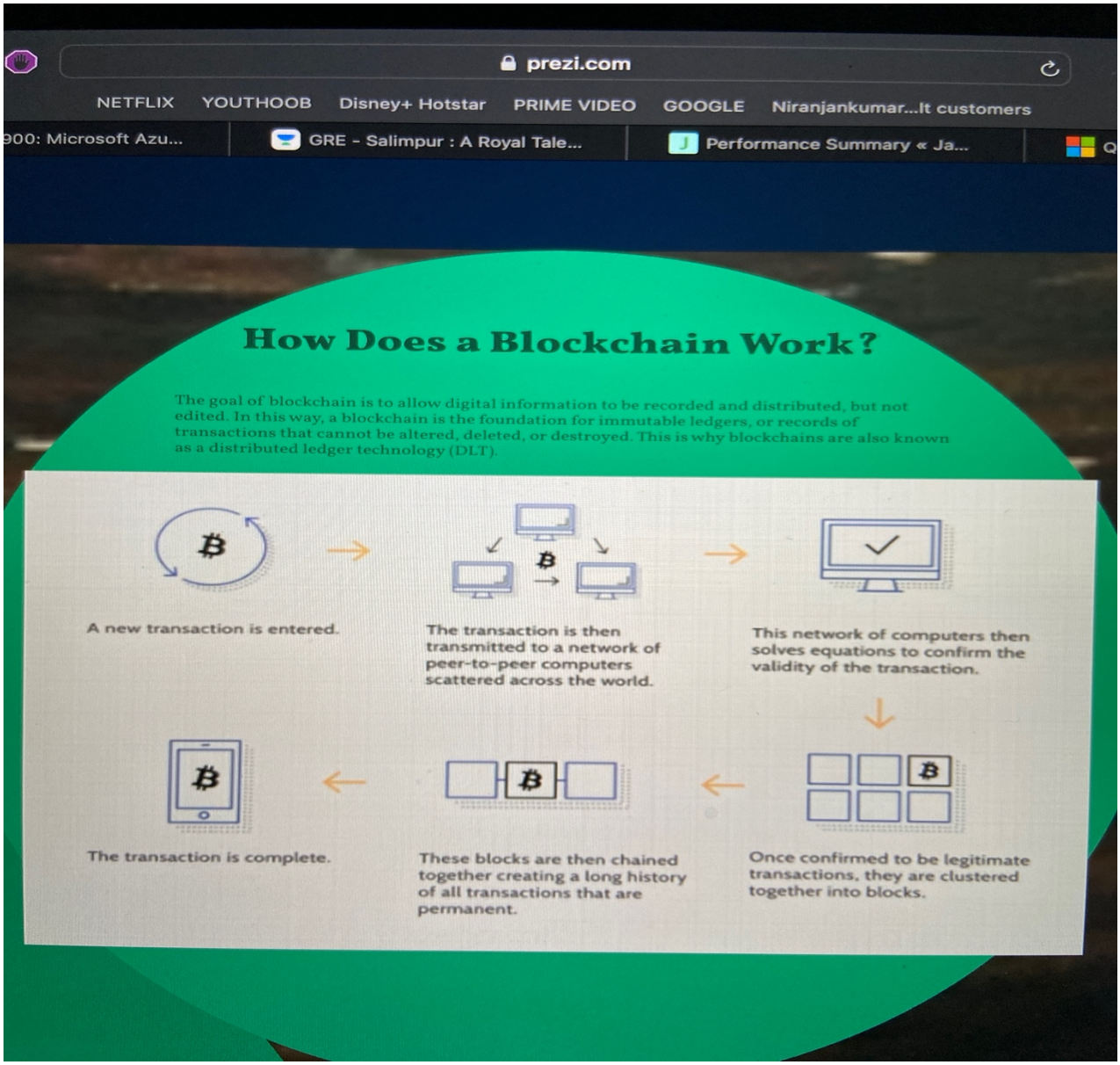
One of the inherent limitations of smart contracts is that the underlying blockchain they run on are isolated networks, meaning blockchains have no built-in connection to the outside world. Without external connectivity, smart contracts cannot communicate with external systems to confirm the occurrence of real-world events nor can they access cost-efficient computational resources. Similar to a computer without the Internet, smart contracts are extremely limited without real-world connectivity. For example, they can't know the price of an asset before
executing a trade, they can't check the average monthly rainfall before paying out a crop insurance claim, and they cannot verify that goods have arrived before settling with a supplier • Thus, the major evolution underway in the blockchain industry is programmable smart contracts that connect with real-world data and traditional systems outside a blockchain, expanding the inputs and out puts used within smart contract logic. These hybrid smart contracts use secure middleware known as an oracle to combine on-chain code with off-chain infrastructure e.g., trigger a smart contract with external data or settle a contract off-chain on a traditional payment rail.

What Is a Blockchain?

A blockchain is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blocks in stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party. One key difference between a typical database and a blockchain is how the data is structured. A blockchain collects information together in groups, known as blocks, that hold sets of information. Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled. With many practical applications for the technology already being implemented and explored, blockchain is finally making a name for itself in no small part because of bitcoin and cryptocurrency. As a buzzword on the tongue of every investor in the nation, blockchain stands to make business and government operations more accurate, efficient, secure, and cheap, with fewer middlemen.
As we prepare to head into the third decade of blockchain, it's no longer a question of if legacy companies will catch on to the technology--it's a question of when. Today, we see a proliferation of NFTs and the tokenization of assets. The next decades will prove to be an important period of growth for blockchain

How does a blockchain work?

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. In this way, a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed. This is why blockchains are also known
as a distributed ledger technology (DLT).

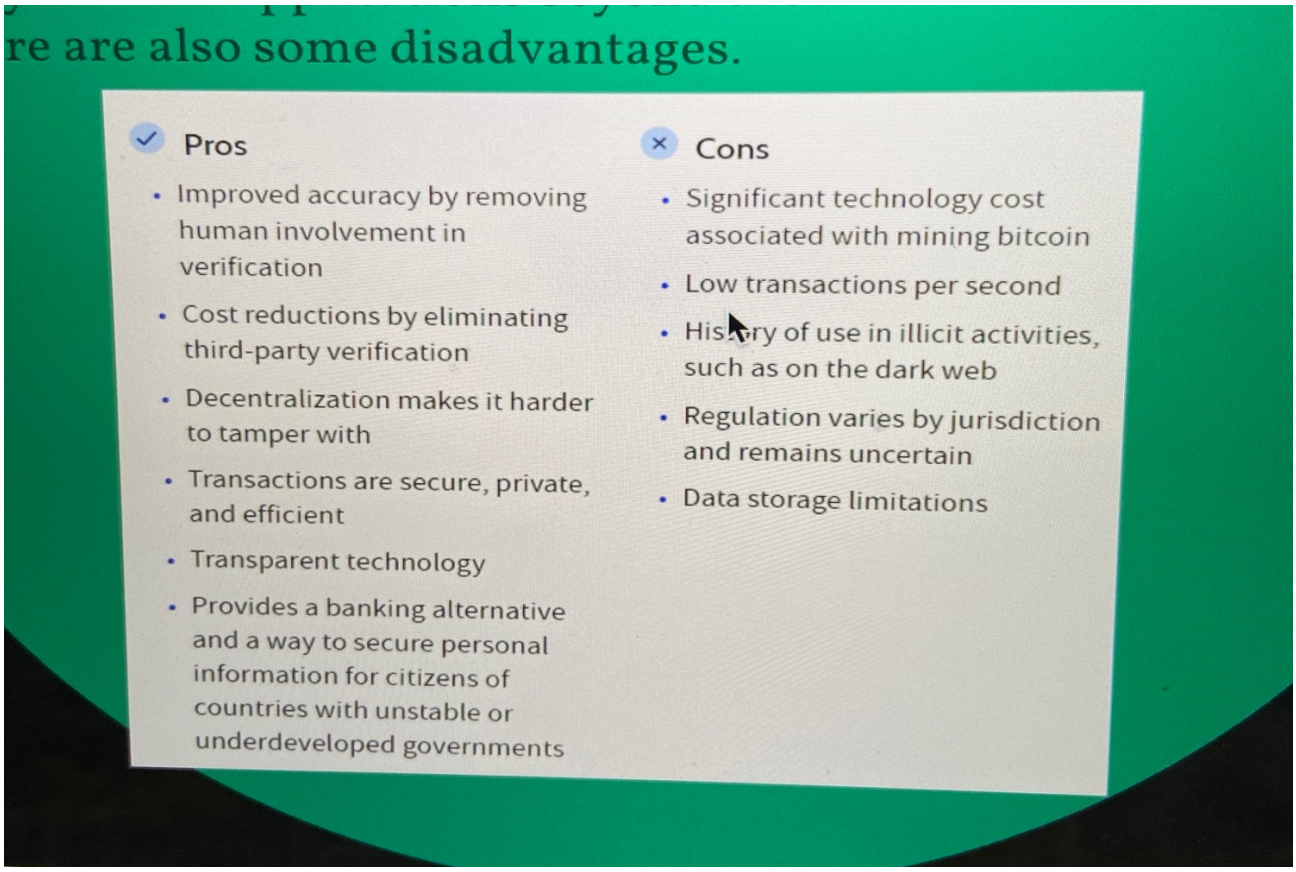


BLOCK CHAIN DECENTRALISATION:

what a blockchain does is to allow the data held in that database to be spread out g several network nodes at various locations. This not only creates redundancy so maintains the fidelity of the data stored therein- if somebody tries to alter r at one instance of the database, the other nodes would not be altered and could prevent a bad actor from doing so. If one user tampers with Bitcoin's d of transactions, all other nodes would cross-reference each other and easily pint the node with the incorrect information. This system helps to establish an and transparent order of events. This way, no single node within the network information held within it. use of this, the information and

history (such as of transactions of a to currency) are irreversible. Such a record could be a list of transactions (such that cryptocurrency), but it also is possible for a blockchain to hold a variety of information like legal contracts, state identifications, or a company's product.

PROS AND CONS:



ORACLE-
Problems w Blockchain:

Since the blockchain has its distributed ledger nature, each node in the network has to be able to find the same end result given the same input. Otherwise, when a node looks to validate a transaction another node makes, it would end up with a different result. This architecture is intentional, and it's designed to be deterministic intentionally, In blockchain, the mechanism for agreeing upon a data value is called consensus, and determinism is important so that nodes can come to a consensus. You might have heard of some of them, like Proof of Work (PoW) with Nakamoto Consensus or Proof of Stake (PoS) with Byzantine Consensus. Consensus is

one of the key ingredients that make blockchain work in the first place. But we need the blockchain world to connect with the real world. We need to get the price of ETH and other cryptocurrencies into a contract so we can have DeFi. We need to get the weather data so we can have decentralized trust less insurance. We need data to use blockchain for one of its most important purposes, smart contracts. So how do we bridge the worlds with this constraint?

Solution:

A blockchain oracle is any device or entity that connects a deterministic blockchain with off-chain data. These oracles enter every data input through an external transaction. This way, we can be sure that the blockchain itself contains all of the information required to verify itself. This is why oracles are known as blockchain middleware: They are the bridge between the two worlds. What is a decentralized oracle? A decentralized oracle or decentralized oracle network is a group of independent blockchain oracles that provide data to a blockchain. Every independent node or oracle in the decentralized oracle network independently retrieves data from an off-chain source and brings it on-chain. The data is then aggregated so the system can come to a deterministic value of truth for that data point. Decentralized oracles solve the oracle problem. Chain-link is a framework for choosing your independent network of nodes to connect the real world's data to the blockchain to enable smart contracts to reach their true potential. With this, we are leveraging the same reliable decentralized infrastructure concept the blockchain has, but for blockchain oracles. If nodes/ sources are hacked, depreciated, or deleted, the network of Chain-link will leverage the decentralized network and carry on. A blockchain oracle is any device or entity that connects a deterministic blockchain with off-chain data. These oracles enter every data input through an external transaction. This way, we can be sure that the blockchain itself contains all of the information required to verify itself. This is why oracles are known as blockchain middleware: They are the bridge between the two worlds.

What is a decentralized oracle?

A decentralized oracle or decentralized oracle network is a group of independent blockchain oracles that provide data to a blockchain. Every independent node or oracle in the decentralized oracle network independently retrieves data from an off-chain source and brings it on-chain. The data is then aggregated so the system can come to a deterministic value of truth for that data point. Decentralized oracles solve the oracle problem. Chain-link is a framework for choosing your independent network of nodes to connect the

real world's data to the blockchain to enable smart contracts to reach their true potential. With this, we are leveraging the same reliable decentralized infrastructure concept the blockchain has, but for blockchain oracles. If nodes/ sources are hacked, depreciated, or deleted, the network of Chain-link will leverage the decentralized network and carry on

POW - Proof of Work:

The proof of work (PoW) is a common consensus algorithm used by the most popular cryptocurrency networks like bitcoin and Litecoin. It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain. However, this whole mining mechanism of bitcoin needs high energy consumption and a longer processing time.

Understanding Proof of Work

This explanation will focus on proof of work as it functions in the bitcoin network. Bitcoin is a digital currency that is underpinned by a kind of distributed ledger known as a "blockchain." This ledger contains a record of all bitcoin transactions, arranged in sequential "blocks," so that no user is allowed to spend any of their holdings twice. In order to prevent tampering, the ledger is public, or "distributed"; an altered version would quickly be rejected by other users.
The way that users detect tampering in practice is through hashes, long strings of numbers that serve as proof of work. Put a given set of data through a hash function (bitcoin uses SHA-256), and it will only ever generate one hash. Due to the "avalanche effect," however, even a tiny change to any portion of the original data will result in a totally unrecognizable hash. Whatever the size of the original data set, the hash generated by a given function will be the same length. The hash is a one-way function: it cannot be used to obtain the original data,
only to check that the data that generated the hash matches the original data.

POS - proof of stake:

The proof of stake (PS) is another common consensus algorithm that evolved as a low-cost, low-energy consuming alternative to the PoW algorithm. It involves the allocation of responsibility in maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens held by it. However, this comes with the drawback that it incentivizes crypto coin hoarding instead of spending. proof-of-stake reduces the amount of computational work needed to verify blocks and transactions that keep the blockchain, and thus a cryptocurrency, secure, Proof-of-stake changes the way blocks are verified using the machines of coin owners. The owners offer their coins as collateral for the chance to validate blocks. Coin owners with staked coins become "validators." Validators are then selected randomly to "mine," or validate the block. This system randomizes who gets to "mine" rather than using a competition-based mechanism like proof-of-work. To become a validator, a coin owner must 'stake" a specific amount of coins. For instance, Ethereum will require 32 ETH to be staked before a user can become a validator. Blocks are validated by more than one validator, and when a specific number of the validators verify that the block is accurate, it is finalized and closed. Different proof-of-stake mechanisms may use different methods for validating blocks--when Ethereum transitions to PoS, it will use shards for transaction submissions. A validator will verify the transactions and add them to a shard block, which requires at least 128 validators to attest to. Once shards are validated and block created, two-thirds of the validators must agree that the transaction is valid, then the block is closed.

DIFFERENCE B/W POW AND POS:

Both consensus mechanisms help blockchains synchronize data, validate information and process transactions. Each method has proven to be successful at maintaining a blockchain, although there are pros and cons to each. However, the two algorithms has very differing approaches.
Under PoS, block creators are called validators. A validator checks transactions, verifies activity, votes on outcomes, and maintains records.
Under PoW, the creators are called miners. Miners solve complex mathematical problems to verify transactions; in return To "buy into" the position of becoming a block creator, investors need only to purchase the sufficient limit of coins or tokens required to become a validator for a PoS blockchain. For PoW, miners must invest in processing equipment and incur heavy energy charges to power the machines attempting to solve the computations. The equipment and energy cost under PoW mechanisms are

expensive, limiting access to mining and strengthening the security of the blockchain. However, PoS blockchains often allow for more scalability due to their energy efficiency.

SOLIDITY - EVM:

The Ethereum Virtual Machine (or) EVM is a virtual stack that is embedded within every fully participating node in the network, or Ethereum node, that executes contract bytecode. The EVM is a Turing complete system, which means it can perform any type of logical step associated with computational functions While Bitcoin provides rewards for running a transaction, Ethereum charges fees for executing software instructions. The gas mechanism in Ethereum lets users pre-pay for the instructions they want to execute on the EVM using Ether, its native currency. EVMs are pretty versatile in that they can be implemented using JavaScript, C++, Ruby, Python, and a variety of other languages.
The contracts that are run using the EVM are written using Solidity. So, once and for all, what is Solidity? It is a high-level programming language that is compatible with how humans express instructions - using numbers and letters instead of binary code Solidity smart contracts are instructions that are then compiled to the EVM's bytecode. The nodes in the Ethereum network, as mentioned, run EVM instances that permit them to agree on the execution of the same set of instructions.

DLT - DISTRIBUTED LEDGERS

PROPERTIES:

1. **Programmable:** A blockchain is programmable (i.e., smart contracts)
2. **Distributed:** All network participants have a copy of the ledger for complete transparency.
3. **Immutable:** Any validated records are irreversible and cannot be changed
4. **Time-Stamped:** A transaction stamp is recorded on a block
5. **Unanimous:** All network participants agree to the validity of each of the records
6. **Anonymous:** The identity of participants is either anonymous or pseudonymous.

7. **Secure**

Blockchain is one type of a distributed ledger. Distributed ledgers use independent computers (referred to as nodes) to record, share and synchronize transactions in their respective electronic ledgers (instead of keeping data centralized as in a traditional ledger).

• This could address persistent challenges in the financial sector and change roles of financial sector stakeholders. DIT has the potential to transform various other sectors as well, like manufacturing, government financial management systems and clean energy. • Since this technology is still nascent, the World Bank Group doesn't have general recommendations about its use for international development. We are in dialogue with standard-setting bodies, governments, central banks and other stakeholders to monitor, research and pilot applications based on blockchain and DIT. • However, waiting for "perfect" DIT solutions could mean missing an opportunity to help shape it. To understand how DLT can address challenges in the financial sector requires both research and real-life applications and pilots. legal, regulatory and technological issues that arise with the advent of new technology. • DLT applications will likely be incremental, and will likely first replace processes and activities that are still manual and inefficient. (Such as reference data maintenance in payment and settlement systems, trade finance, syndicated loans, and tracking provenance of agricultural products and commodities, their subsequent sale or use as financing collateral.) • Eventually, DLT could increase efficiency and lower remittance costs, and potentially improve access to finance for unbanked populations, who are currently outside the traditional financial system. • Messages based on WBG's fintech note on Distributed Ledger Technology and Blockchain, published December 2017.

DAPP - Decentralised Application:

A decentralized app (also known as a dApp or dapp) operates on a blockchain or peer-to-peer network of computers. It enables users to engage in transactions directly with one another as opposed to relying on a central authority. Dapps have their backend code (smart contracts) running on a decentralized network and not a centralized server. They use the blockchain for data storage and smart contracts for their app logic.
A smart contract is like a set of rules that live on-chain for all to see and run exactly according to those rules. Imagine a vending machine: if you supply it

with enough funds and the right selection, you'll get the item you want. And like vending machines, smart contracts can hold funds much like your blockchain account. This allows code to mediate agreements and transactions, Once dapps are deployed on the Blockchain network you can't change them. Dapr can be decentralized because they are controlled by the logic written into the contract, not an individual or a company.

PROPERTIES:

A dapp can have frontend code and user interfaces written in any language (just like an app) to make calls to its backend. Furthermore, its frontend can get hosted on decentralized storage such as IPFS.

Decentralized - dapps operate on Ethereum, an open public decentralized platform where no one person or group has control

Deterministic - dapps perform the same function irrespective of the environment in which they get executed

Turing complete - dapps can perform any action given the required resources

Isolated - dapps are executed in a virtual environment known as Ethereum Virtual Machine so that if the smart contract has a bug, it won't hamper the normal functioning of the blockchain network On smart contracts

IPFS - INTERPLANTARY FILE SYSTEM:

The Interplanetary File System (IPFS) is a protocol and peer-to-peer network for storing and sharing data in a distributed file system A dapp can have frontend code and user interfaces written in any language (just like an app) to make calls to its backend. Furthermore, its frontend can get hosted on decentralized storage such as IPFS. Here's what happens when you add a file to IPFS - whether you're storing that file on your own local node or one operated by a pinning service or IPFS-enabled app.

I) When you add a file to IPFS, your file is split into smaller chunks, cryptographically hashed, and given a unique fingerprint called a content identifier (CID). This CID acts as a permanent record of your file as it exists at that point in time.

2) When other nodes look up your file, they ask their peer nodes who's storing the content referenced by the file's CID. When they view or download your file, they cache a copy - and become another provider of your content until their cache is cleared.

3)A node can pin content in order to keep (and provide) it forever, or discard content it hasn't used in a while to save space. This means each node in the network stores only content it is interested in, plus some indexing information that helps figure out which node is storing what.

4 If you add a new version of your file to IPFS, its cryptographic hash is different, and so it gets a new CID. This means files stored on IPFS are resistant to tampering and censorship - any changes to a file don't overwrite the original, and common chunks across files can be reused in order to minimize storage costs.

5)However, this doesn't mean you need to remember a long string of CIDs - IPFS can find the latest version of your file using the IPNS decentralized naming system, and DNSLink can be used to map CIDs to human-readable DNS names.

BENEFITS :

Zero downtime - Once the smart contract is deployed on the blockchain, the network as a whole will always be able to serve clients looking to interact with the contract. Malicious actors, therefore, cannot launch denial-of-service attacks targeted towards individual dapps.

Privacy - You don't need to provide real-world identity to deploy or interact with a dapp.

Resistance to censorship - No single entity on the network can block users from submitting transactions, deploying dapps, or reading data from the blockchain.

Complete data integrity - Data stored on the blockchain is immutable and indisputable, thanks to cryptographic primitives. Malicious actors cannot forge transactions or other data that has already been made public.

Trust less computation/verifiable behaviour - Smart contracts can be

analysed and are guaranteed to execute in predictable ways, without the need to trust a central authority. This is not true in traditional models; for example, when we use online banking systems, we must trust that financial institutions will not misuse our financial data, tamper with records, or get hacked.

ISSUES:

Maintenance - Dapps can be harder to maintain because the code and data published to the blockchain are harder to modify.

Performance overhead - There is a huge performance overhead, and scaling is really hard. To achieve the level of security, integrity, transparency, and reliability that Ethereum aspires to, every node runs and stores every transaction.

Network congestion - When one dapp uses too many computational resources, the entire network gets backed up. Currently, the network can only process about I0-15 transactions per second.

User experience - It may be harder to engineer user-friendly experiences because the average end-user might find it too difficult to set up a tool stack necessary to interact with the blockchain in a truly secure fashion.

Centralization - User-friendly and developer-friendly solutions built on top of the base layer of Ethereum might end up looking like centralized services anyways.