UNIT II

BLOCKCHAIN TECHNOLOGY

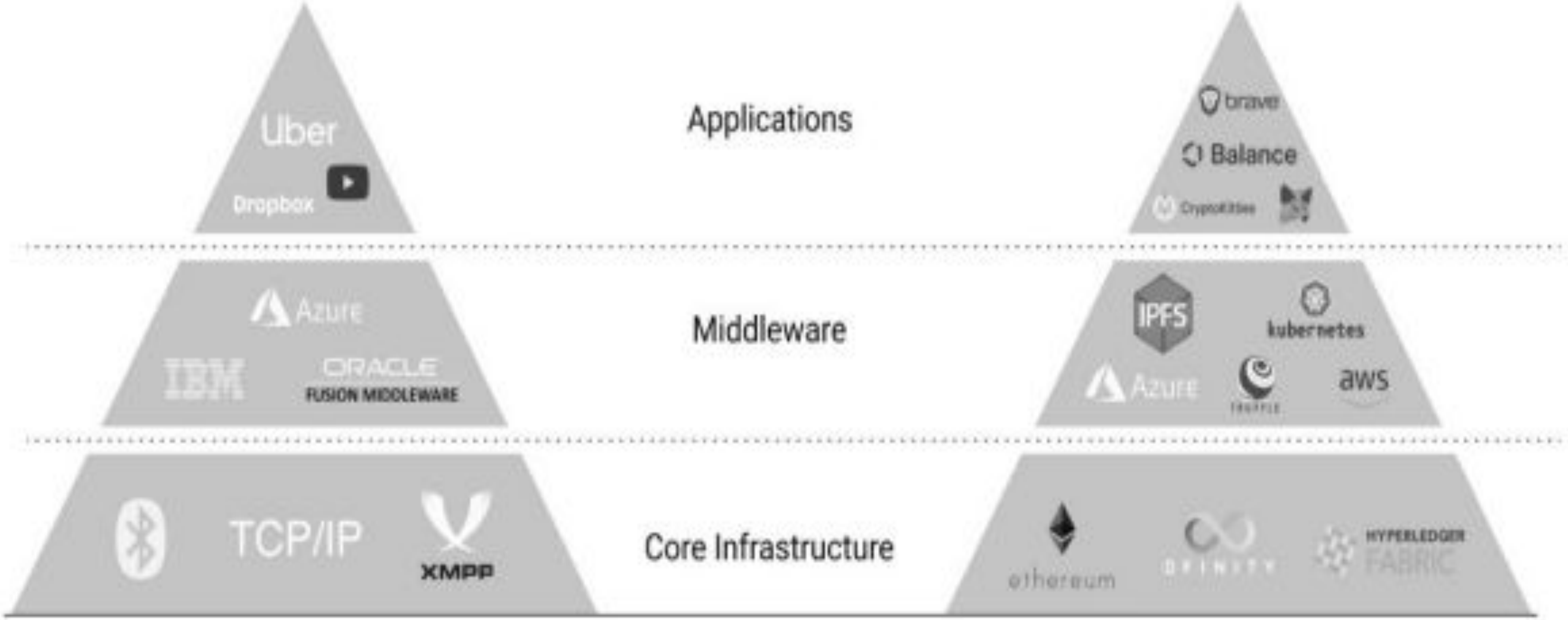
Internet Stack

- Our Internet has three major layers:
- 1. **Core infrastructure layer:** This layer consists of general protocols like TCP/IP (Transmission Control Protocol / Internet Protocol) that helps establish the communication between computers and the network architecture.
- **2. Middleware layer:** Middleware refers to a set of tools, dev-tech, and services that make application development faster and easier. They function as a hidden translation layer between an operating system and the applications on top.
- Content Management Systems (CMS), query languages, web servers, and application servers were developed as early middleware for our Internet in order to enable publishing and managing text and imagery online (e.g. Websites). Other middleware examples are database access services, web-middleware, messaging middleware, or transaction-processing monitors

Internet Stack (Contd.)

- **3. Application layer:** Built on top of core infrastructure and middleware live applications. These are the tools and products you are likely used to using such as Gmail or Uber, etc.

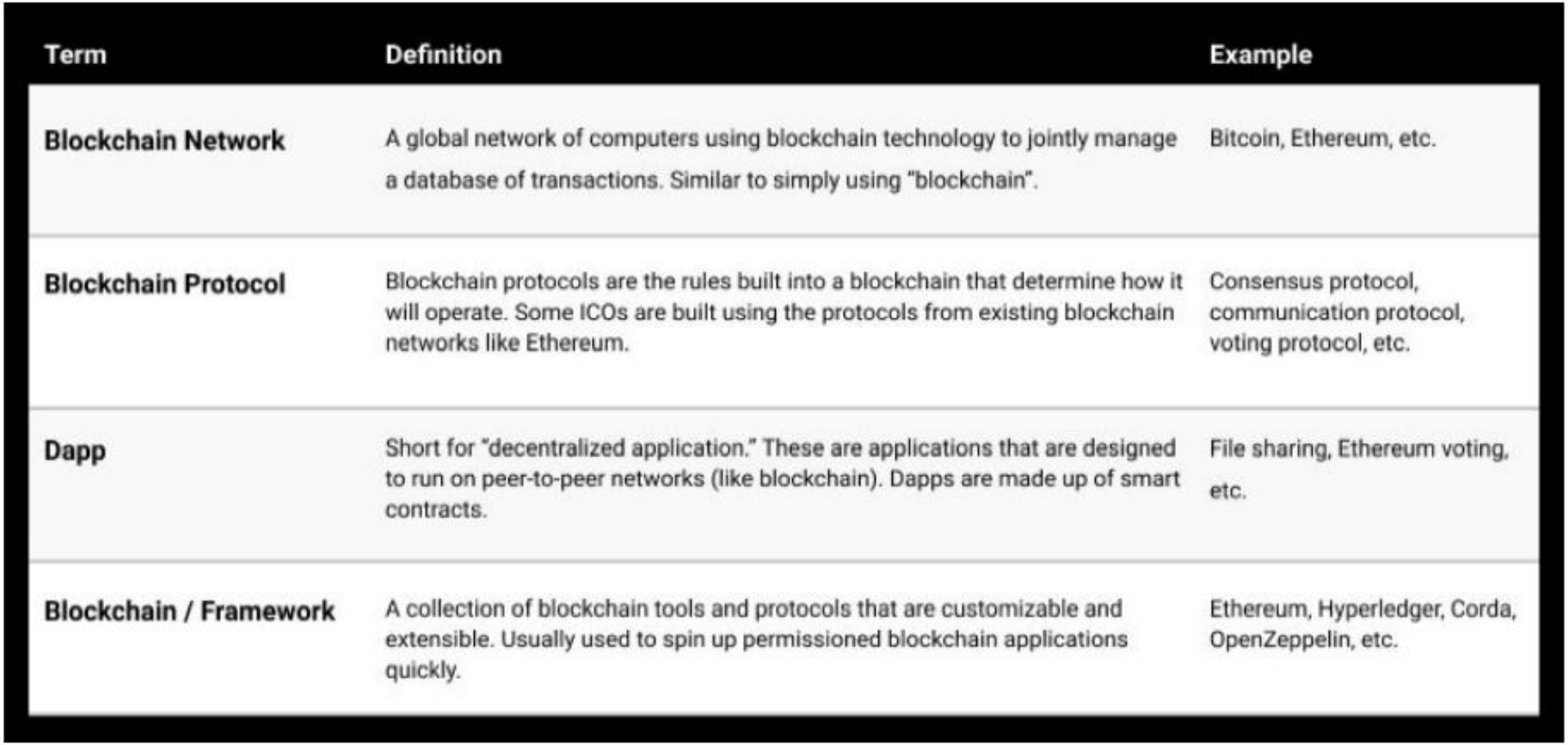
Comparison of Internet and Blockchain Stack



- The **bottom layer**, or **core infrastructure** of a blockchain, is made up of a complex piece of software that is typically programmed in JavaScript, C ++, Python, or Go.
- It is a mashup of different functions, called **protocols**, which define behaviors for communication and transaction on the network.
- This includes software that allows for the creation and listing of nodes on the network, and their ability to communicate via a peer-to-peer network protocol.
- Since each node functions as both a client and a server, this means that each node must have the ability to store and retrieve files.

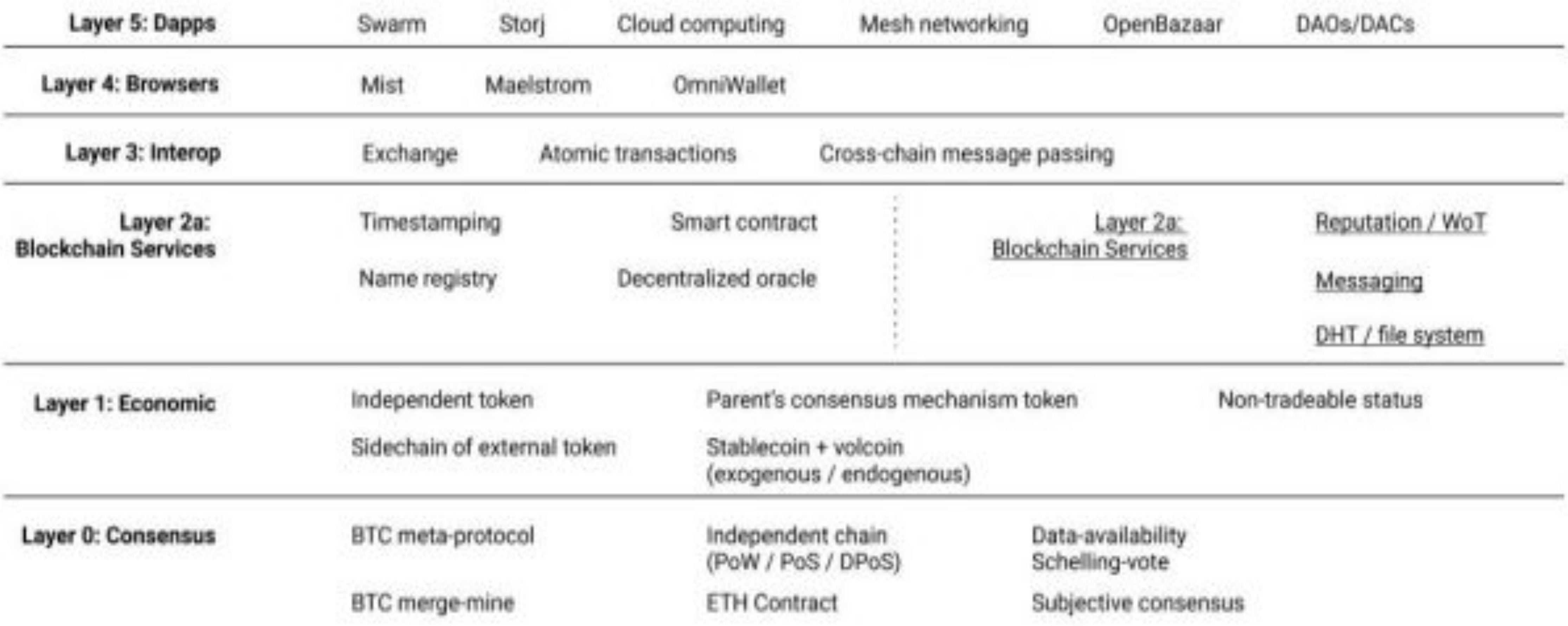
- A **server** is a connection point for handling client requests such as getting data, while a **client** is software that allows a user to connect to a server and make a request for some kind of service, like retrieving a file.
- Being able to both store and retrieve files is crucial since core blockchain protocols rely on nodes being able to store a complete copy of the entire blockchain.
- The software is not an operating system but makes use of GNU (popular free software operating system) capabilities and TCP/IP Internet protocols to allow different types of devices running different operating systems to communicate across the network.
- Also built into the software are rules for creating new blocks using **consensus** (i.e. Proof of Work and longest chain rule) and rules for how the blocks will be secured via encryption.

- The most established blockchains are **permissionless networks**, which means that anyone can participate and install the blockchain software from the open-source community.
- This is often done from **open-source software repositories.**
- By installing the software and downloading the blockchain, you are not necessarily running a “full node” on the blockchain and your node is not yet monetizable.
- Running a node on a blockchain only becomes monetizable when the node agrees to participate in the contest to actively maintain the security of the blockchain by joining the **“community of verifiers.”**
- In the world of the Ethereum blockchain and its smart contracts, this means that full nodes additionally store and run individual smart contracts.
- Depending on the way the core blockchain protocols are configured, a full node might be considered to be a “miner” and would be rewarded with the native digital token (bitcoin, ether, etc.) for winning the competition to create a block and for verifying the transactions that were collected into the block. Both the smart contract layer as well as the storage and content layer describe platforms for developing blockchain-based applications.



Term	Definition	Example
Blockchain Network	A global network of computers using blockchain technology to jointly manage a database of transactions. Similar to simply using "blockchain".	Bitcoin, Ethereum, etc.
Blockchain Protocol	Blockchain protocols are the rules built into a blockchain that determine how it will operate. Some ICOs are built using the protocols from existing blockchain networks like Ethereum.	Consensus protocol, communication protocol, voting protocol, etc.
Dapp	Short for "decentralized application." These are applications that are designed to run on peer-to-peer networks (like blockchain). Dapps are made up of smart contracts.	File sharing, Ethereum voting, etc.
Blockchain / Framework	A collection of blockchain tools and protocols that are customizable and extensible. Usually used to spin up permissioned blockchain applications quickly.	Ethereum, Hyperledger, Corda, OpenZeppelin, etc.

Figure 2-2: Table of blockchain terminology



Layer 5: Dapps	Swarm	Storj	Cloud computing	Mesh networking	OpenBazaar	DAOs/DACs
Layer 4: Browsers	Mist	Maelstrom	OmniWallet			
Layer 3: Interop	Exchange	Atomic transactions	Cross-chain message passing			
Layer 2a: Blockchain Services	Timestamping Name registry	Smart contract Decentralized oracle	Layer 2a: Blockchain Services	Reputation / WoT Messaging DHT / file system		
Layer 1: Economic	Independent token Sidechain of external token	Parent's consensus mechanism token Stablecoin + volcoin (exogenous / endogenous)	Non-tradeable status			
Layer 0: Consensus	BTC meta-protocol BTC merge-mine	Independent chain (PoW / PoS / DPoS) ETH Contract	Data-availability Schelling-vote Subjective consensus			

Figure 2-3: The many layers of blockchain

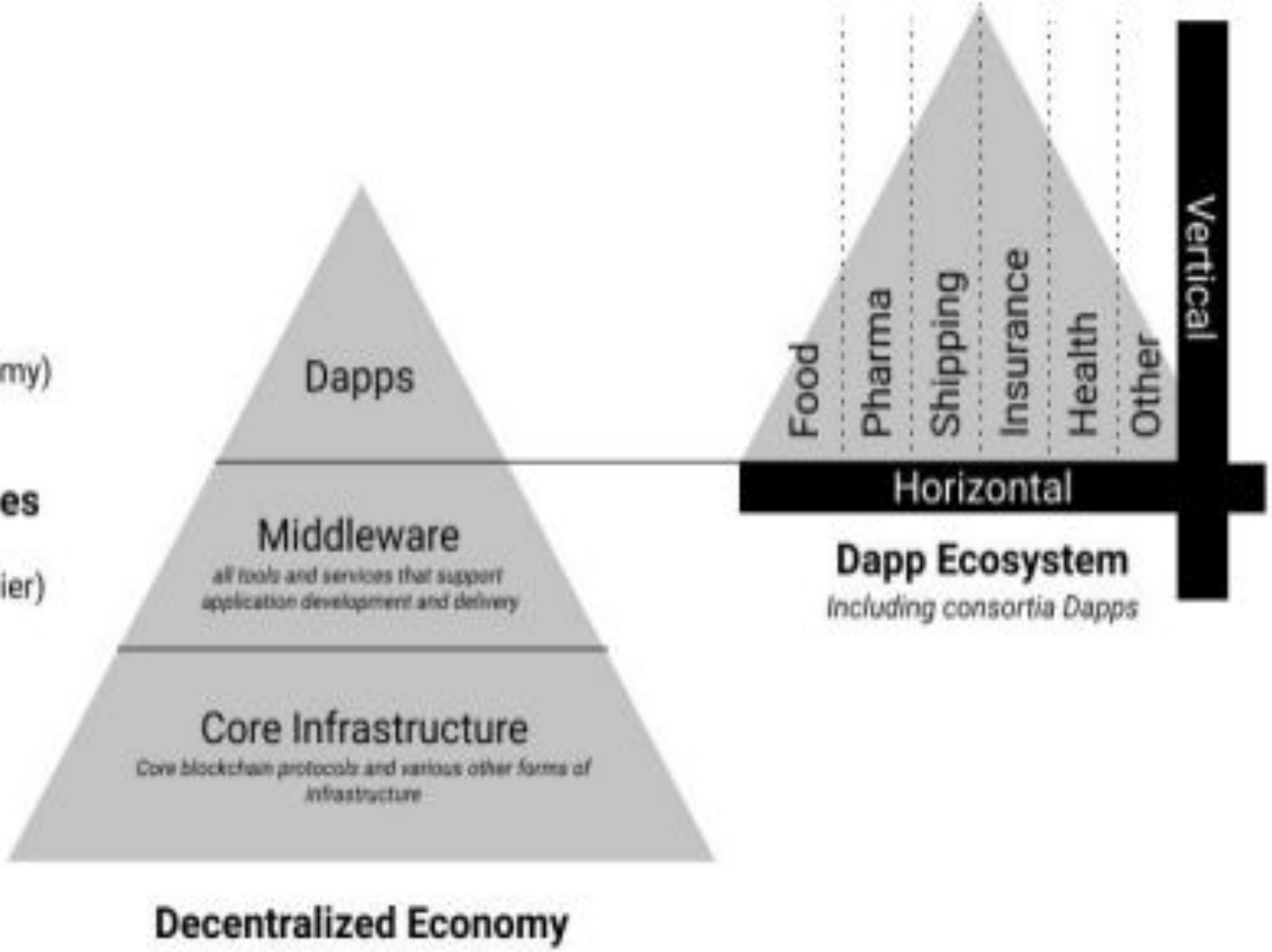
Monetizing The Blockchain

- Monetizing the Core Infrastructure
- Monetizing Middleware
- Monetizing the Decentralized Economy

Monetize products & services
(e.g. similar kind of apps exist in digital economy)

Monetize developer tools and services
(e.g. tools and technologies that
makes Dapp development faster, cheaper, easier)

Monetize network crypto-assets
(e.g. bitcoin, ether, etc.)


Dapps
Middleware
all tools and services that support application development and delivery
Core Infrastructure
Core blockchain protocols and various other forms of infrastructure
Decentralized Economy
Food
Pharma
Shipping
Insurance
Health
Other
Vertical
Horizontal
Dapp Ecosystem
Including consortia Dapps

1. Monetizing Core Infrastructure

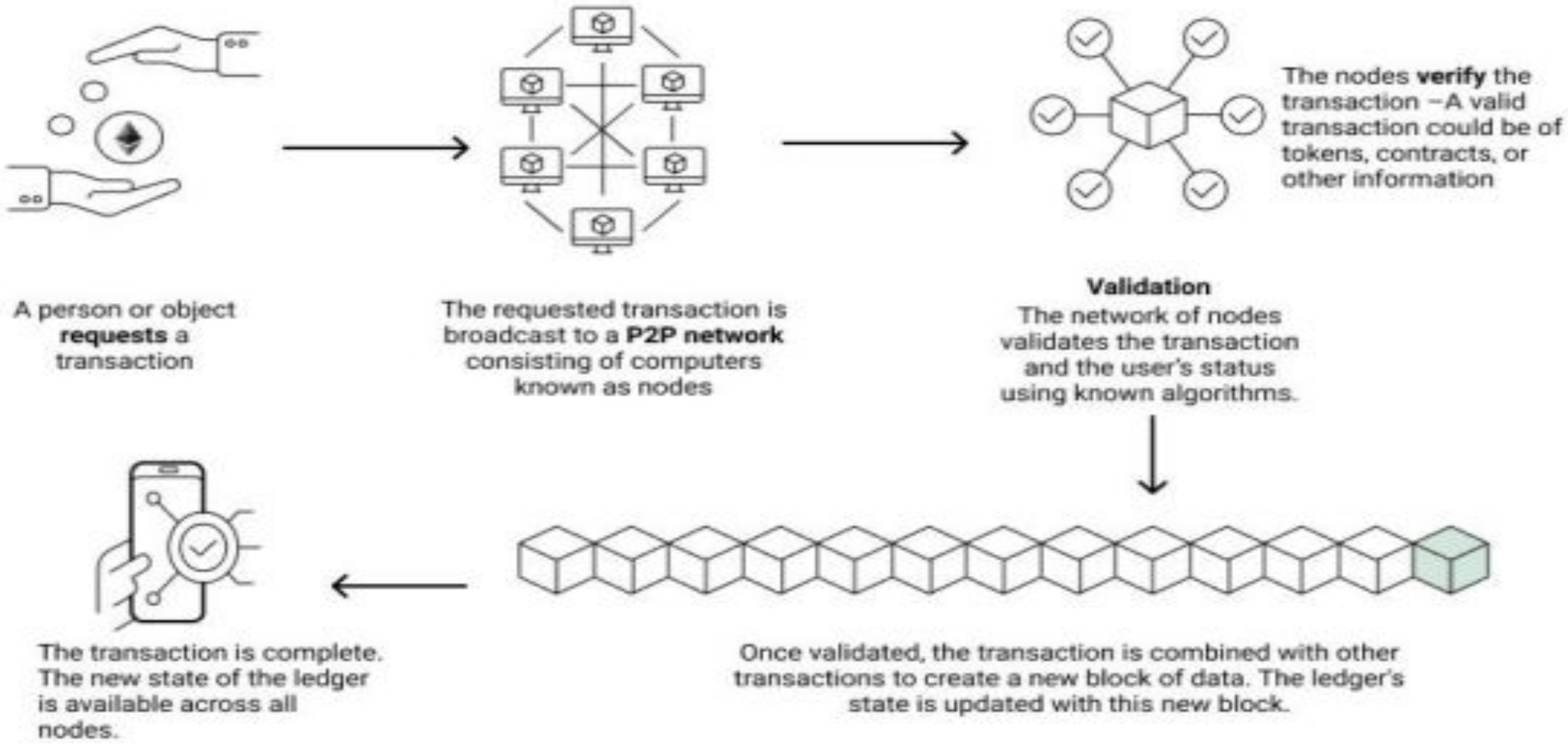
- **Digital tokens** are a key component of blockchain technology.
- To motivate people to participate in a blockchain as a full node and help secure the history of transactions, blockchains include **tokens** as part of an **incentive structure.**
- A digital token simply represents a value on a blockchain network. Tokens for blockchain networks come in many shapes and sizes, and people are experimenting with how to codify and incentivize participants in blockchains through token-based economic frameworks.

1. Monetizing Core Infrastructure (Contd.)

- Bitcoin and ether can be considered examples of **“intrinsic”** or **“native”** digital tokens since each is built into its network.
- These tokens only exist as entries in a blockchain ledger and must be reached with a user’s private key in order to receive any value for them.
- There are many other types of digital tokens and the number grows every day.
- One example: so-called **“stablecoins”** that are pegged to a fiat currency (like a USD or Euro). Some of the most popular stablecoins today are USD Coin (USDC), Dai (DAI), and Tether (USDT) which are all slightly different in their conception.
- The main monetization opportunity at the network core infrastructure layer is tied to the idea that greater usage of a given blockchain (e.g. more transaction volume, more middleware, and applications, etc.) will drive greater value of its token underlying token due to network effects.

1. Monetizing Core Infrastructure (Contd.)

- The ability to create value at the **network core infrastructure** through tokens is one of the reasons many groups have launched new blockchains with their own digital tokens.
- The main monetization opportunity at the network core infrastructure layer is tied to the idea that **greater usage of a given blockchain** (e.g. more transaction volume, more middleware and applications, etc.) will drive greater value of its token underlying token due to network effects.



A person or object **requests** a transaction

The requested transaction is broadcast to a **P2P network** consisting of computers known as nodes

The nodes **verify** the transaction –A valid transaction could be of tokens, contracts, or other information

Validation
The network of nodes validates the transaction and the user's status using known algorithms.

Once validated, the transaction is combined with other transactions to create a new block of data. The ledger's state is updated with this new block.

The transaction is complete. The new state of the ledger is available across all nodes.

Figure 2-5: Diagram of transactions on a blockchain

2. Monetizing Middleware

- The smart middleware layer is a logical extension of the original token concept.
- The goal of achieving a peer-to-peer network for transacting value can go beyond financial value and tokens and include transactions that are basic functions that a computer can perform.
- **The middleware layer of a blockchain technology stack is one of the areas where we are starting to see more experimentation because with the growth of middleware for any core infrastructure comes benefits, such as reduced complexity, improved efficiency, and an increase in application development.**

2. Monetizing Middleware (Contd.)

- For example, the Internet's application layer started to flourish only after both cost and risk of application development diminished because of new middleware solutions.
- Today's blockchain networks are just starting to see middleware development.
- **For instance, the Truffle suite exists for the Ethereum network, making it easier to build decentralized applications on top of Ethereum.**
- Various middleware solutions are being built with smart contracts and are monetizable products or services.
- If we compare blockchain middleware tools and services to those of the digital economy, there are similar opportunities: **content management and storage, query languages, etc.**

3. Monetizing Decentralized Economy

- The decentralized application layer of the technology stack is where the majority of economic activity will take place.
- This is where we see use-case solutions: **products, applications, and services.**
- Decentralized applications are made up of **smart contracts – essentially, software that encodes business logic or governance.**
- Almost any current application that exists in our digital economy can be re-imagined as a product or service in the decentralized economy built on blockchain technology.
- Consumers can interact with specific Dapps that sit on top of the blockchain stack which take advantage of **asset tracking, identity management, and so forth.**

Blockchain Wallet

- Blockchain wallets provide individual users the ability to transact on a blockchain network directly.
- To have a wallet essentially means that you have an account on a particular blockchain network.
- This account provides access to other network participants and the Dapps on top of the network itself.
- Each account is assigned an immutable account-based identity, (a public key) through which to interact with Dapps and other users.
- One could almost compare a blockchain wallet to a credit bank account.
- The main difference with blockchain wallets, however, is that there is no centralized body determining your creditworthiness or other banking activities – that is done by other network participants.

- **A blockchain wallet, also known as a cryptocurrency wallet, is a digital wallet that allows users to store, send, and receive cryptocurrencies such as Bitcoin, Ethereum, and others. Unlike traditional wallets, which hold physical cash and cards, blockchain wallets store cryptographic keys that provide access to the user's cryptocurrency holdings on the respective blockchain network.**
- **1. Storage of Private Keys:** Blockchain wallets store a user's private keys, which are cryptographic keys that provide access to their cryptocurrency funds. These private keys are used to sign transactions and prove ownership of the associated cryptocurrency assets.
- **2. Public Addresses:** Each blockchain wallet has one or more public addresses associated with it. These addresses are derived from the wallet's public key and are used to receive cryptocurrency payments. Users can share their public addresses with others to receive funds.
- **4. Security Considerations:** Users need to take steps to secure their blockchain wallets, such as enabling two-factor authentication (2FA), using strong passwords, and keeping private keys secure. Hardware wallets are generally considered the most secure option for storing large amounts of cryptocurrency.
- **5. Backup and Recovery:** Users should also create backups of their wallet's private keys or recovery phrases (also known as seed phrases). This ensures that they can regain access to their funds in case their wallet is lost, stolen, or inaccessible.

- 3. **Types of Wallets:** There are different types of blockchain wallets, including:
- - **Software Wallets:** These wallets are software applications that run on desktop computers, smartphones, or tablets. Examples include Coinbase Wallet, MetaMask, and Trust Wallet.
- - **Hardware Wallets:** These wallets are physical devices that securely store private keys offline. They are considered more secure than software wallets because they are immune to malware attacks. Examples include Ledger Nano S, Trezor, and KeepKey.
- **- Paper Wallets:** A paper wallet is a physical document that contains a user's public and private keys printed on paper. It's considered a form of cold storage and provides offline security.
- **- Web Wallets:** These wallets are hosted on a website or online service and can be accessed through a web browser. They are convenient but may be less secure than other types of wallets due to the risk of hacking.
- - **Exchange Wallets:** Cryptocurrency exchanges often provide wallets for their users to store their funds on the exchange platform. However, storing cryptocurrency on exchanges carries some security risks, as users do not have full control over their private keys.

Blockchain Wallet (Contd.)

- Blockchain wallets are essential to participation in a blockchain network.
- Each blockchain network has its version of a wallet.
- A wallet helps your computer to function as a **"virtual machine."**
- Your blockchain virtual machine is a higher abstraction than your computer itself.
- One way of thinking of a "virtual machine" or VM is to think of it as a special area within your computer either on your hard drive or in the cloud, where you can run different operating systems and applications.
- You may have partitioned your hard drive in the past so you could run both Windows applications and Mac applications on your computer.
- It is a similar concept for our virtual machine on the blockchain network. **It is what allows you to function as a node on a blockchain and run the programs that you need to use to access the functionality of your blockchain.** All of this happens separately from other applications running on your computer that might conflict with the global virtual machine running the entire blockchain.

Blockchain Wallet (Contd.)

- If you were to use a wallet on the Ethereum blockchain network, you can be an account owner of ether (the crypto-asset), you can work as a miner that provides computing power to the underlying network, and you can be a Dapp participant (by making transactions using smart contracts).
- If you have a specific wallet say, for bitcoin, keep in mind that the wallet doesn't actually store bitcoin in it. What is stored is your public key, which is also known as your bitcoin address. This is a string of 34 letters and numbers. This address is stored in a table which links up to a complete history of all transactions that are linked to this address.
- When a miner validates a transaction, all it has to do is look up the public address in order to make sure that there is enough bitcoin in that wallet to complete the transaction and that it hasn't been spent already. Since no one necessarily knows the identity of the person behind any given wallet, it does not matter if the whole network sees a wallet's contents and transactions.
- Your wallet address/public key has a corresponding "private key" of 64 letters and numbers. Given the encryption, no one can reverse engineer your public key in order to find out your private key.
- Most cases of hacking involve people being tricked into giving out their private keys or if funds are stored within an exchange (i.e. you do not control your own wallet). When Ava tells her wallet to pay Barry she must "sign" the transaction using the private key stored on her computer or smartphone. The digital signature gets sent to the network where it is validated as corresponding to the public key for the account.

Blockchain Wallet (Contd.)

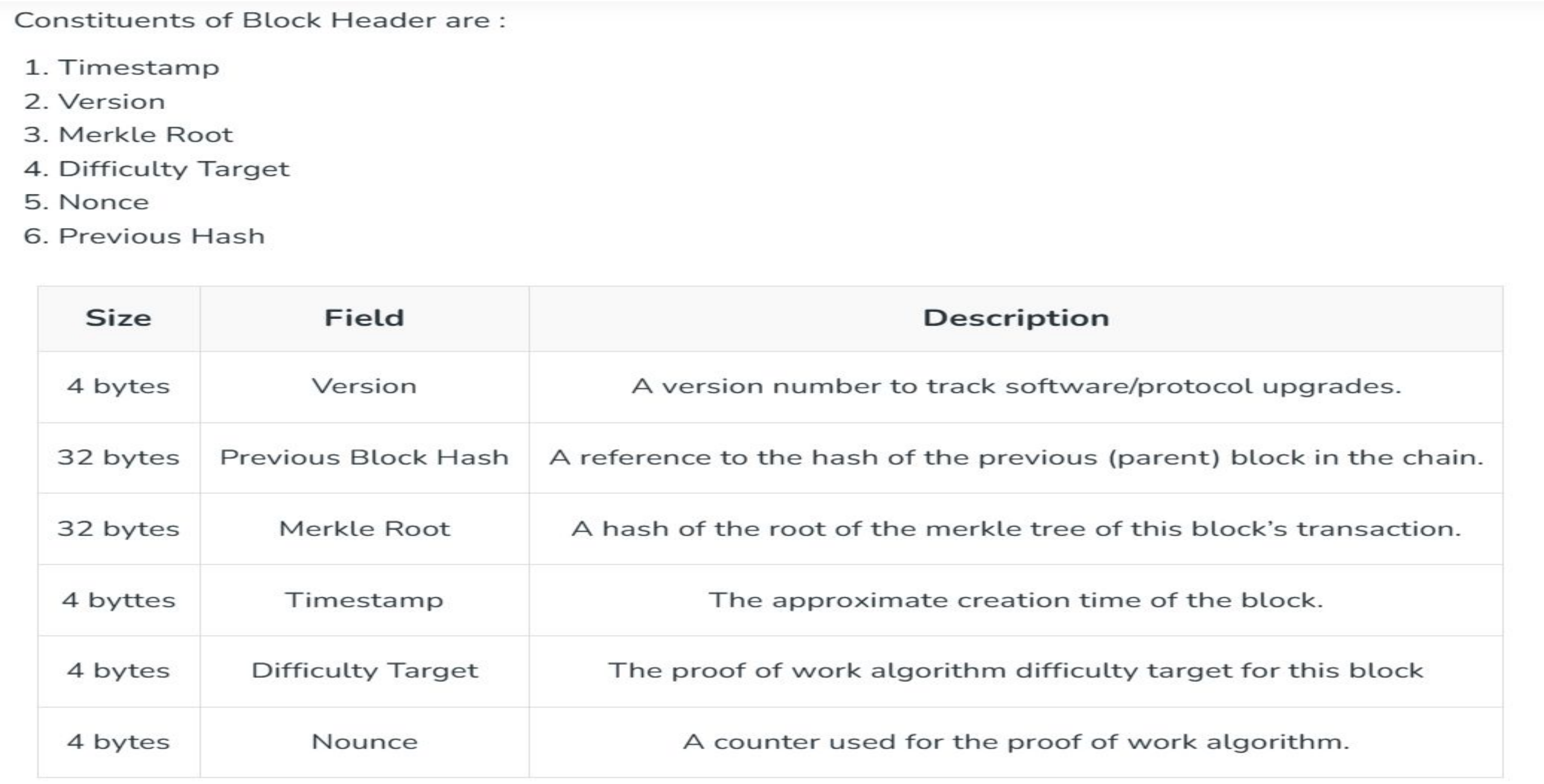
- When someone decides that they wish to use bitcoin or some other cryptocurrency, the first thing they must do is to choose a wallet.
- Like physical wallets, there is a wide variety of these available to the consumer. Most cryptocurrency exchanges have their own wallets that the user can download and install from the exchange website. These may be dedicated wallets only for bitcoin, or they may allow the storage of additional coins. Most of these are web-based wallets and don’t require the user download the entire Bitcoin Core.
- Some people who buy and sell lots of cryptocurrencies store the bulk of their coins in **“cold storage.”** These options are called cold storage because they do not require a continuous connection to a server on the Internet in order to gain access to them. Thus, if someone were to gain access to your wallet, you wouldn’t lose all of your digital assets. And cold storage is less susceptible to hacking, too. The simplest form of cold storage is printing out your public and private keys or QR codes in order to create a “paper wallet.”
- The biggest advancement in wallet technology has come in the form of **“hardware wallets.”** These are generally recommended today since they are highly secure for storing private keys and are not continuously connected to the Internet. They are considered to be immune to software viruses and malware. **Trezor** makes one of the most popular hardware wallets

Sorting Blocks

- When a digital ledger gets to a certain size, a protocol in its blockchain software determines that it is time to create a new block.
- Storing transactions in blocks makes it easier to search and manage the huge number of transactions created and stored on the blockchain.
- This is equivalent to the shared ledger that is copied to all of the nodes on the peer-to-peer network.
- The full nodes race to create the new block because they want to collect the transaction fees and also the full reward for creating the block. Keep in mind that every blockchain network (Bitcoin, Ethereum) or Dapp will operate a completely separate shared ledger.

Sorting Blocks (Contd.)

- In creating a new block, a node generates a unique identifier or block header for that block which will be used to identify it when it eventually gets chained into the blockchain’s history.
- The block header will contain a hash of all the transactions in the block.
- As a reference point, **in the case of Bitcoin, a block header is 80 bytes long.**
- To ensure that the identifier is unique the nodes participate in a mathematical game that uses a cryptographic hash algorithm (SHA-256) to generate a unique hash for the entire block.
- **By design, the size of each block in the Bitcoin network is about 1 MB and it will take roughly 10 minutes to create a new block. Different blockchains arrive at consensus in different ways.**
- Many use a Proof of Work mechanism for Sybil attack resistance, combined with other protocols, and some new ones are moving to a Proof of Stake technique and even Proof of Elapsed Time



Constituents of Block Header are :

1. Timestamp
2. Version
3. Merkle Root
4. Difficulty Target
5. Nonce
6. Previous Hash

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades.
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain.
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transaction.
4 byttes	Timestamp	The approximate creation time of the block.
4 bytes	Difficulty Target	The proof of work algorithm difficulty target for this block
4 bytes	Nounce	A counter used for the proof of work algorithm.

Rewarding Miners

- In any of the blockchain platforms, one of the miners or validators has to validate a payment transaction and then add it to a new valid block, so how is that miner rewarded?
- By finding the valid block hash for the new block, the miner has provided a “proof of work” which means he/she has invested in the **electricity and computing resources** needed to find the block hash.
- This essentially ties a real monetary cost to the mining process just like in mining for precious metals.
- As computing power grows, the difficulty can be increased by requiring more zeroes or even letters to be found using the nonce.
- This can be seen in the “difficulty” parameter in Figure 2-14 where it was set to only four zeroes.

Rewarding Miners (Contd.)

- When a miner has found a winning block hash, the miner announces this to the entire network and when 51% of the miners validate the block hash, a reward is deposited in that miner’s wallet.
- According to the Bitcoin protocol, miners currently receive 12.5 bitcoin in addition to the total value of the transaction fees for all the transactions contained in that block.
- Originally, the reward was set at 50 bitcoin, but it has been cut in half every four years; first to twenty-five and now to 12.5 bitcoin.
- As the reward keeps decreasing, the miners will have to rely more on higher transaction fees in order to pay for the costs of mining.

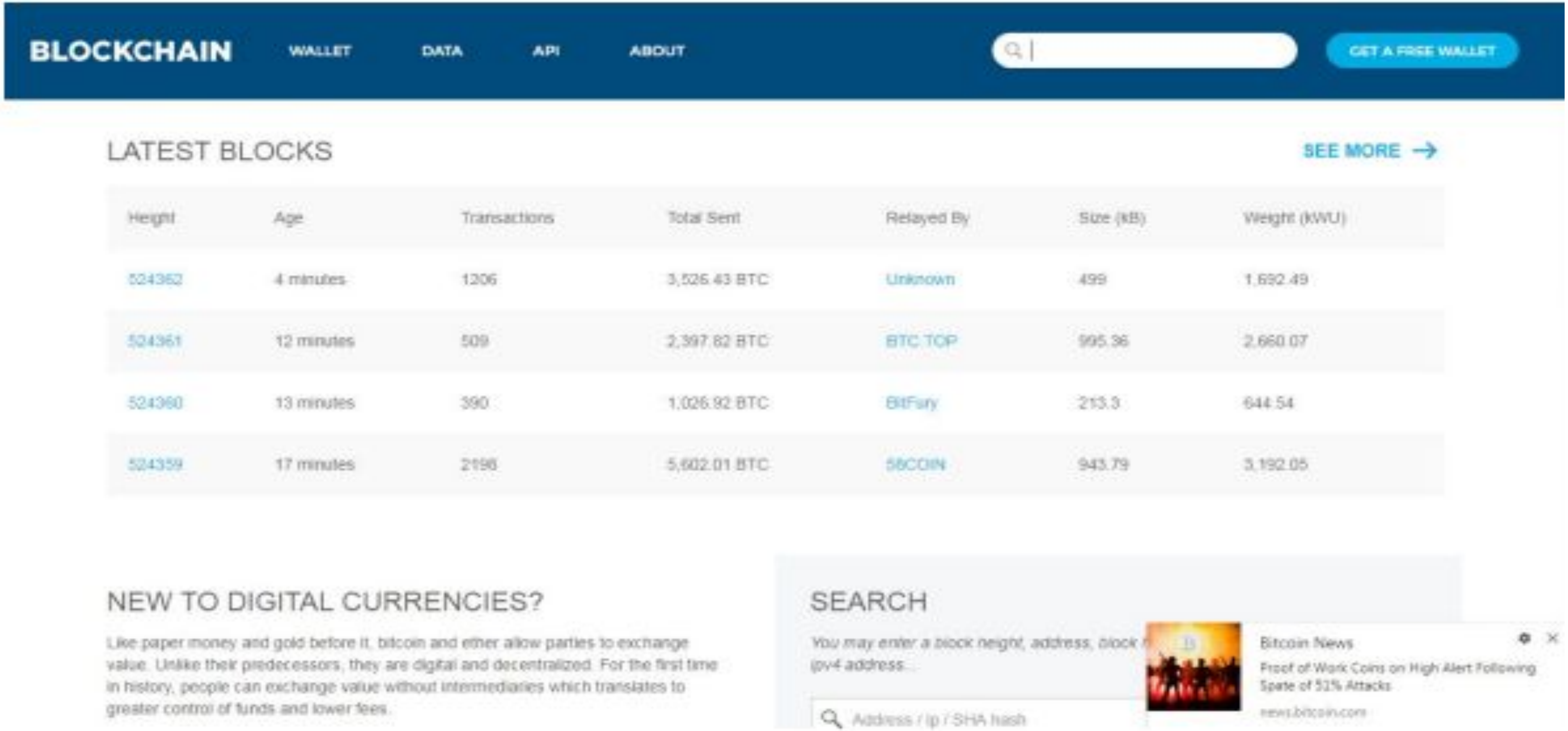
Consensus

- When you download blockchain software and become a full node on a network, this means that you can participate in generating a consensus among all of the nodes.
- In the case of Bitcoin, the consensus rules of the network determine how the participants in the network interact with each other. They define:

1. The **conditions** under which a transaction (i.e. sending tokens from party A to party B) are valid.
2. The **transaction costs** related to sending money from party A to party B.
3. The **incentive mechanism** for validating transactions with a digital token.
4. **Rules** of how to change current consensus rules.

Consensus (Contd.)

- The rules of consensus can vary widely between blockchain networks and can also be changed.
- This can be extremely difficult to do or relatively simple depending on the blockchain network's governance and core protocols.
- They are optimized for key qualities like **privacy, throughput, and scalability.**



LATEST BLOCKS

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
524362	4 minutes	1206	3,526.43 BTC	Unknown	499	1,692.49
524361	12 minutes	509	2,397.82 BTC	BTC.TOP	995.36	2,660.07
524360	13 minutes	390	1,026.92 BTC	BitFury	213.3	644.54
524359	17 minutes	2198	5,602.01 BTC	58COIN	943.79	3,192.05

NEW TO DIGITAL CURRENCIES?

Like paper money and gold before it, bitcoin and ether allow parties to exchange value. Unlike their predecessors, they are digital and decentralized. For the first time in history, people can exchange value without intermediaries which translates to greater control of funds and lower fees.

SEARCH

You may enter a block height, address, block h ipv4 address...

Bitcoin News

Proof of Work Coins on High Alert Following Spate of 51% Attacks

news.bitcoin.com

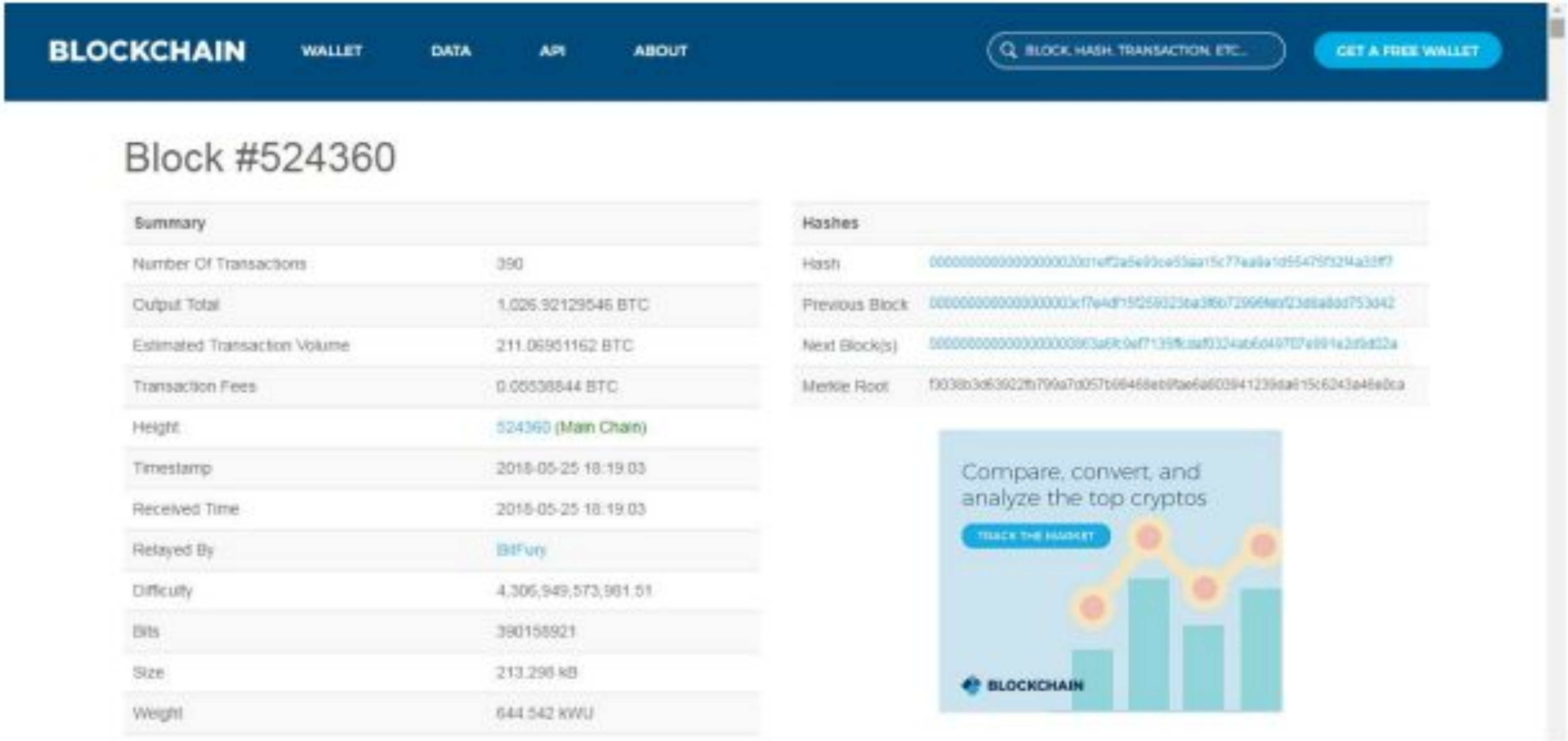
Figure 2-14: Block creation data

Consensus (Contd.)

- The data on the Bitcoin blocks is readily available for anyone to see.
- This figure shows the current block being created along with the data on the last three blocks that were created.
- The time (age) it took to mine these three blocks varies quite a bit as does the number of transactions contained in the block.
- This is because it is not possible to predict how long it will take to generate the winning hash value or the final block content of the winning block.
- It also shows here the amount of bitcoin sent in each of the transactions and who was the successful miner of each block, displayed in the “relayed by” field.
- Most of the blocks are close to 1 MB of data, but this can vary too.

Consensus (Contd.)

- The height of the block refers to the number of blocks that came before the current block. If you look at the genesis block mined by Satoshi (see Figure 2-16), you can see that it has a height of “0” since it was the first block.
- The block “weight” refers to the size in terms of the amount of memory that the block takes up.
- The kWU stands for thousands of weight units or roughly equivalent to megabytes of memory.
- The weight varies quite a bit too, though the maximum was raised to 4 kWU or about 4 MB in order to try and increase the volume of transactions processed in each block.



Block #524360

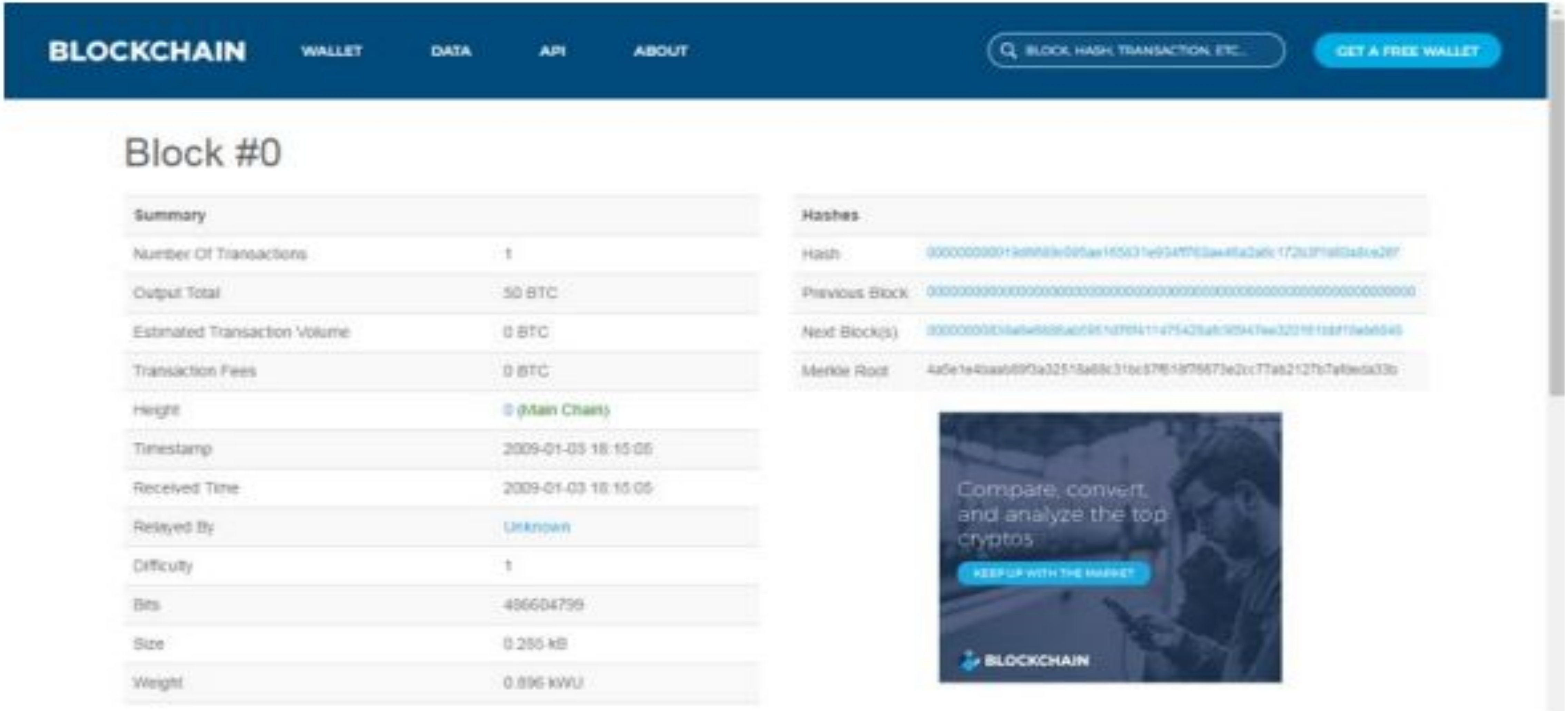
Summary	
Number Of Transactions	390
Output Total	1,026.92129546 BTC
Estimated Transaction Volume	211.06951162 BTC
Transaction Fees	0.05538844 BTC
Height	524360 (Main Chain)
Timestamp	2018-05-25 18:19:03
Received Time	2018-05-25 18:19:03
Relayed By	BitFury
Difficulty	4,306,949,573,981.51
Bits	390158921
Size	213.298 kB
Weight	644.542 KWU

Hashes	
Hash	000000000000000000020d1eff2a5e93ce53aa15c77ea8a1d55475f32f4a33ff7
Previous Block	000000000000000000003cf7e4df15f259323ba3f6b72996fabf23d8a8dd753d42
Next Block(s)	0000000000000000000003863a6fc0af7139ffcdaf0324ab6d49707e891a2d9d02a
Merkle Root	f3038b3d63922fb799a7d057b69468eb9fae6a603941239da615c6243a46e0ca

Figure 2-15: Block details

Consensus (Contd.)

- Figure 2-15 shows the **number of transactions** contained in the block, the amount of bitcoin involved in the transactions along with the transaction fees collected by the successful miner, in this case, BitFury.
- The **time-stamp** is a crucial piece of metadata because it shows when the block was created and validated.
- This may be important since other miners are competing to be the first to solve the cryptographic hashing problem and create the new block.
- With the time-stamp, BitFury can prove that they solved the problem first and therefore are entitled to the **reward and the transaction fees**. You can also see the hash value of this block and the previous block, along with the Merkle root, difficulty, height, and weight.



Block #0

Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU

Hashes	
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Figure 2-16: Bitcoin genesis block

Blockchain as a Service (BaaS)

- Blockchain as a Service (BaaS) is a cloud-based service that enables users to develop, host, and operate blockchain applications and functions without the complexity of building and maintaining the infrastructure typically associated with blockchain technology.
- 1. **Infrastructure Management:** With BaaS, the infrastructure required to run a blockchain network is managed by a service provider. This means users don't have to worry about setting up servers, storage, or networking for their blockchain applications.
- 2. **Development Tools:** BaaS providers often offer tools and APIs (Application Programming Interfaces) that make it easier for developers to build and deploy blockchain applications. These tools can include smart contract templates, SDKs (Software Development Kits), and other development resources.
- **3. Scalability and Flexibility:** BaaS solutions typically offer scalability features that allow blockchain networks to handle a growing number of transactions and users. Additionally, users can often choose from different blockchain platforms and configurations based on their specific needs.

Blockchain as a Service (BaaS)

- 4. **Cost-Efficiency:** By using BaaS, organizations can reduce the costs associated with building and maintaining their own blockchain infrastructure. They can also benefit from a pay-as-you-go pricing model, where they only pay for the resources and services they use.
- 5. **Security**: BaaS providers often implement security measures to protect the blockchain networks hosted on their platforms. This can include encryption, identity management, and other security protocols to safeguard data and transactions.
- 6. **Integration with Other Services:** BaaS can be integrated with other cloud services, such as databases, analytics tools, and IoT (Internet of Things) platforms. This allows organizations to create more comprehensive and interconnected solutions.
- Popular BaaS providers include Microsoft Azure Blockchain, IBM Blockchain Platform, Amazon Managed Blockchain, and Oracle Blockchain Cloud Service, among others.

Blockchain as a Service (BaaS)

- Due to the intense hype around blockchain, many large software firms are racing to deploy a version of blockchain that would take advantage of the cloud to create **“on-demand”** blockchain networks.
- These companies include IBM, Microsoft, SAP, Amazon Web Services, projects like BlockApps, and even the Chinese retail giant Baidu.
- Animal Ventures is launching an open-source platform called Orb Weaver, which allows users to launch a blockchain network on the cloud and provide other services to ease the development of blockchain applications.
- **The basic idea for all these services is that by hosting the blockchain network in the cloud, software companies can help smaller outfits get up and running on a blockchain quickly without the extreme cost of hiring hard-to-find blockchain developers.**
- If you think about the technology stack of a blockchain, the **core layer** is very time-intensive to develop and requires expertise in **kernel development** as well as many other disciplines that come together to define blockchain protocols (economics or game theory, mathematics, cryptography, and computer science, to name a few).

Blockchain as a Service (BaaS) (Contd.)

- Rather than every company trying to prototype or build its own blockchain, BaaS begins to move the prototyping process up into higher parts of the technology stack.
- **This means that companies, especially those whose business is not as technology-heavy, can develop use cases and prototypes for solving specific business pain points through applications of blockchain higher in the stack.**
- Oftentimes, BaaS providers will combine an **enterprise blockchain solution** with a **systems integration solution.**
- The upside of spinning up a blockchain using a BaaS implementation includes lowered needs for talent in development and security at the core layer, decreased time to experimentation, and potentially greater customer support.
- However, outsourcing this work has its downsides as well, including a recentralization of certain functionality, systems lock-in with the chosen provider, as well as the costs of renting the resources to run a hosted blockchain instance.

Information Technology Use Cases for Blockchain

1. **Storage:**

- In the early days of the Internet, a program came along called SETI that sought to leverage all the computers that were connected to the Net but not being used.
- When users downloaded SETI they were volunteering their computing power to run software that would search realms of planetary data for scientific discoveries during the hours that users weren't on their computers.
- We see this kind of model in many places today, through car-sharing apps or even Airbnb: **how can we monetize underutilized resources or incentivize their utilization in new ways?**
- For blockchains, the storage and computing question is an opportunity space that **Dapps like Storj, Sia, Filecoin, and Maidsafe** are attempting to build into leading decentralized storage systems.
- Each of these projects is pushing to improve upon existing storage provider services by reducing costs, improving security, or boosting functionality.
- **These Dapps run on the premise that network users can offer their unused storage capacity across desktops, servers, and storage devices in exchange for tokens.**

Information Technology Use Cases for Blockchain (Contd.)

1. **Storage:**

- **This turns storage into a marketplace, where the nodes that store data receive a reward in return for their service.**
- Companies providing decentralized storage Dapps suggest these services will cost a fraction of what centralized storage platforms are offering and can reinvent everything from consumer tools (e.g Dropbox) to enterprise cloud storage (e.g. Box) on alternate infrastructure.
- The claim that decentralized storage and file management will reduce costs hinges mostly on the potential to reduce inefficiencies such as the hypertext transfer protocol (HTTP) practice of downloading a file from a single computer, rather than many simultaneously.
- The InterPlanetary File System (IPFS) estimates that a peer-to-peer approach to video delivery would reduce bandwidth costs by 60%.

Information Technology Use Cases for Blockchain (Contd.)

1. **Storage:**

- **By decentralizing where and how data is stored, these platforms potentially offer censorship resistance and greater network resiliency.**
- **No central provider could "take down" your data or alter it, and similarly, you could avoid downtime if your business experienced some kind of network failure or cyber-attack, by relying on many independent nodes that store your data.**
- **If privacy is a concern, these solutions suggest the data itself can be split up into small pieces and replicated across the network in a way where no single node or user holds a complete data set.**

Information Technology Use Cases for Blockchain (Contd.)

2. IPFS: IPFS, which stands for InterPlanetary File System, is a distributed protocol designed to create a peer-to-peer (P2P) network for storing and sharing hypermedia and other forms of data.

- Unlike traditional client-server models where data is stored on centralized servers, IPFS aims to decentralize the web by using a distributed network of nodes.

Information Technology Use Cases for Blockchain (Contd.)

2. IPFS:

1. **Content Addressing:** In IPFS, each piece of content is given a unique cryptographic hash called a Content Identifier (CID). This CID is derived from the content itself, which means that if the content changes, its CID will also change. This allows IPFS to detect and prevent data tampering.

2. **Distributed Network**: IPFS operates as a decentralized network of nodes. When a user adds a file to IPFS, it gets divided into smaller chunks, and each chunk is assigned a CID. These chunks are then distributed across multiple nodes in the network.

3. **Peer-to-Peer Communication**: To retrieve content from IPFS, a user's client software (or node) communicates with other nodes in the network using a P2P protocol. It can request specific content by its CID, and the nodes will collaborate to find and retrieve the requested data.

4. **Data Replication:** IPFS uses a data replication strategy known as Content Routing. Nodes in the network maintain a Distributed Hash Table (DHT) to keep track of which nodes are storing specific content. This helps in efficiently locating and retrieving content from the nearest or most available nodes.

5. **Caching and Pinning:** Nodes can cache and pin content they find useful or want to keep available. Caching means temporarily storing data that has been recently accessed, while pinning ensures that specific content remains permanently available on a node.

6. **Security:** IPFS uses cryptographic techniques to ensure data integrity and authenticity. Since each piece of content is uniquely identified by its CID, any alteration to the content will result in a different CID, making it easy to detect tampering. Additionally, data can be encrypted for privacy and security.

7. **Integration with Web Protocols**: IPFS is designed to work alongside existing web protocols like HTTP. This means that content stored on IPFS can be accessed using a standard web browser by resolving IPFS URLs (ipfs://) or through HTTP gateways that translate IPFS addresses to traditional web URLs.

Information Technology Use Cases for Blockchain (Contd.)

2. IPFS:

Benefits of IPFS:

- **Decentralization:** IPFS aims to create a more decentralized and resilient web by distributing content across multiple nodes, reducing reliance on centralized servers.

- **Data Integrity:** With content addressing and cryptographic hashing, IPFS ensures the integrity and authenticity of data.

- **Efficiency:** Content that is frequently accessed can be cached or pinned, improving retrieval times and reducing bandwidth usage.

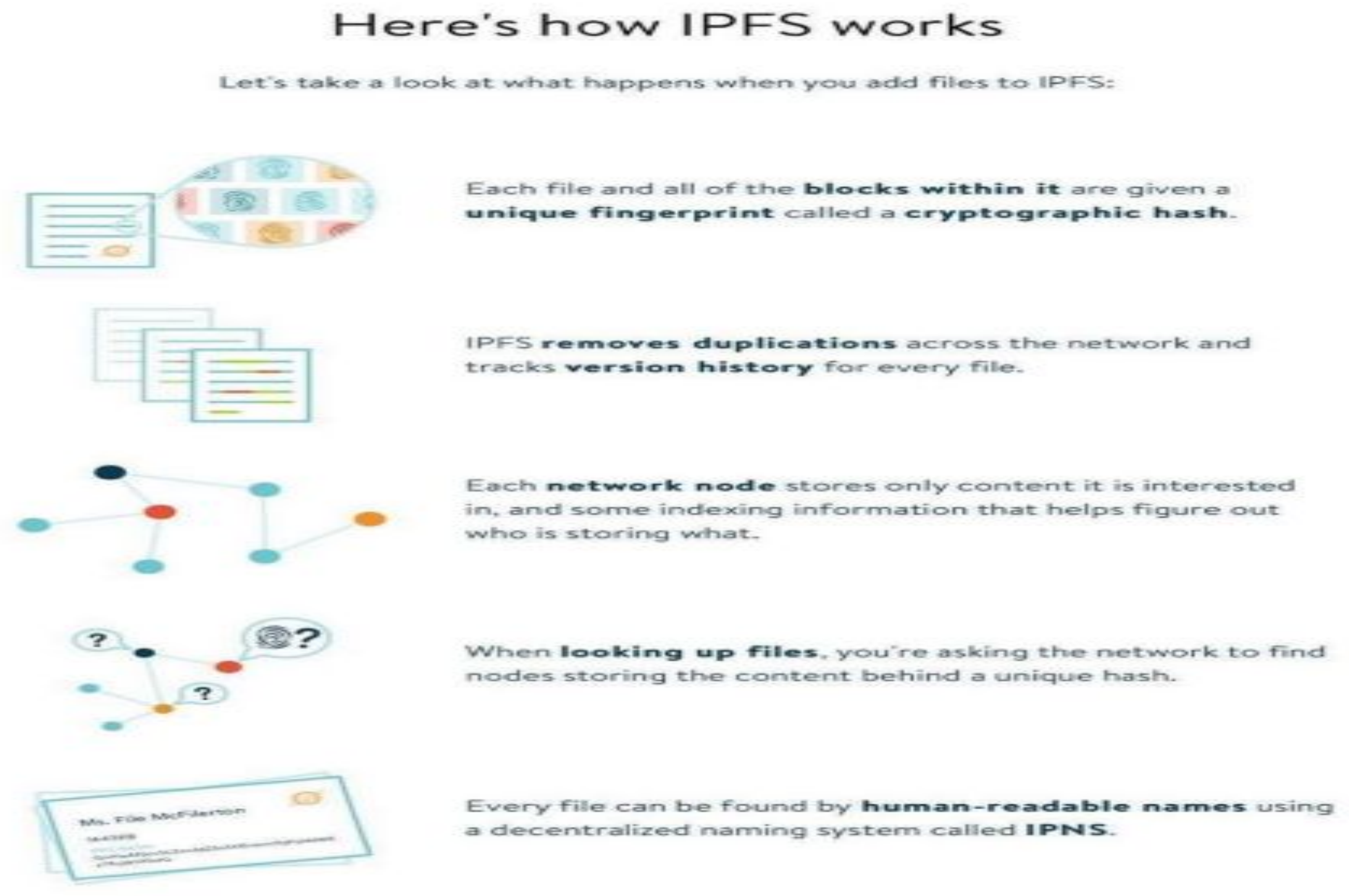
- **Censorship Resistance**: Due to its decentralized nature, IPFS can make it more difficult for authorities or entities to censor or block access to specific content.

Overall, IPFS offers a promising alternative to traditional web hosting and file-sharing methods by leveraging the power of decentralized networks and cryptographic security.

Information Technology Use Cases for Blockchain (Contd.)

2. IPFS

- The InterPlanetary File System (IPFS) is described as a “peer-to-peer” distributed file system that seeks to connect all computing devices with the same system of files.
- In some ways, IPFS is similar to the Web, but IPFS could be seen as a single BitTorrent swarm, exchanging objects within one Git repository.
- The approach is focused on tackling some of the challenges for data distribution, such as computing on large datasets across organizations, hosting and distributing huge datasets, and managing versioning as well as preventing file disappearance.
- Content addressing is an important departure from the way our Web functions today: hyperlinks currently point to addresses not the context of the content. Some examples of using IPFS for websites include inserting videos, pinning, and graphic objects.



Here's how IPFS works

Let's take a look at what happens when you add files to IPFS:

Each file and all of the **blocks within it** are given a **unique fingerprint** called a **cryptographic hash**.

IPFS **removes duplications** across the network and tracks **version history** for every file.

Each **network node** stores only content it is interested in, and some indexing information that helps figure out who is storing what.

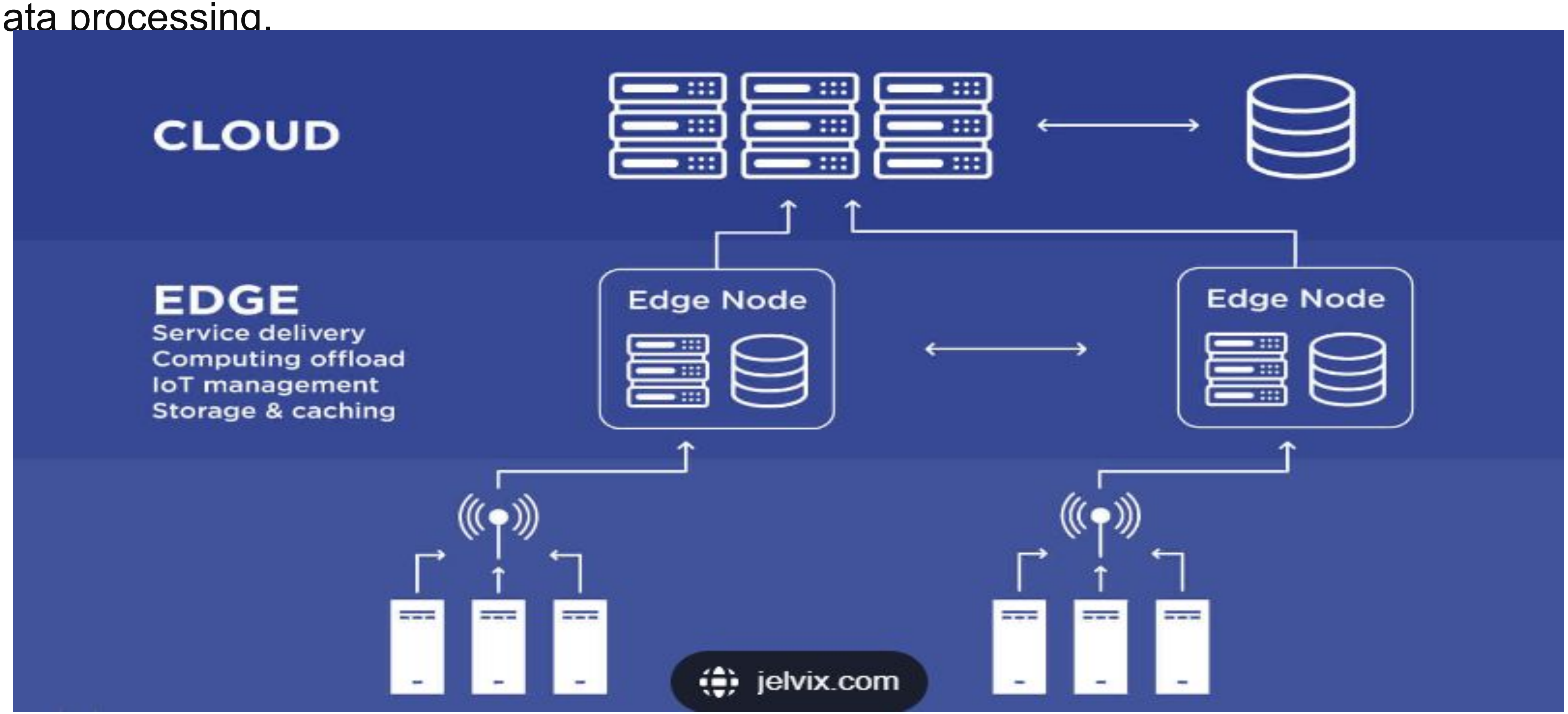
When **looking up files**, you're asking the network to find nodes storing the content behind a unique hash.

Every file can be found by **human-readable names** using a decentralized naming system called **IPNS**.

Figure 2-18: How IPFS works

Information Technology Use Cases for Blockchain (Contd.)

- Edge computing is a distributed computing paradigm that brings computation and data storage closer to the sources of data, such as Internet of Things (IoT) devices or local edge servers. Instead of relying solely on centralized data centers or cloud computing resources, edge computing processes data locally on the device or at the edge of the network, closer to where it is generated. This approach aims to reduce latency, conserve bandwidth, and improve the efficiency and speed of data processing.



Information Technology Use Cases for Blockchain (Contd.)

- Here are some key concepts and characteristics of edge computing:

1. **Low Latency**: By processing data closer to its source, edge computing reduces the time it takes for data to travel between the source and the processing location. This is crucial for applications that require real-time or near-real-time responses, such as autonomous vehicles, industrial automation, and augmented reality/virtual reality (AR/VR).
2. **Bandwidth Efficiency**: Edge computing can help reduce the amount of data that needs to be sent to centralized data centers or the cloud. By filtering and processing data locally, only relevant or summarized data is transmitted, leading to reduced bandwidth usage and costs.
3. **Scalability**: Edge computing can scale easily by adding more edge devices or servers to the network. This allows for distributed computing resources that can handle increasing amounts of data and workload without overloading centralized systems.
4. **Data Privacy and Security**: Processing data locally can enhance data privacy and security. Personal or sensitive data can be processed and stored locally, reducing the risk of data exposure during transit to centralized locations. Additionally, data encryption and secure communication protocols can be implemented at the edge to further protect data.
5. **Reliability**: Edge computing can improve system reliability and resilience by reducing dependence on centralized infrastructure. Local processing can continue to operate even if there is a loss of connectivity to the cloud or centralized data center.
6. **Use Cases**: Edge computing is particularly well-suited for applications and industries that require real-time processing, such as autonomous vehicles, smart cities, healthcare monitoring, industrial automation, retail analytics, and more. It can also be used to enhance content delivery, gaming experiences, and edge AI applications.

- Examples of edge computing technologies and platforms include AWS IoT Greengrass, Microsoft Azure IoT Edge, Google Cloud IoT Edge, and various hardware solutions designed for edge computing tasks.

Information Technology Use Cases for Blockchain (Contd.)

2. Edge Computing:

- **The trajectory of IT development has often been tied to Moore’s Law: the notion that our computing power doubles roughly every 12-18 months.**
- And as our computing power has increased, we have been able to move where and how computing is accomplished.
- Contemporary computational power at the edges of networks and the leveraging of large cloud servers make information technology much more robust.
- **Recent suites of devices that are coming to market allow for computation to be performed locally and then transmitted to the cloud for reference or dissemination across a network.**
- This is one of the most interesting aspects of blockchain technology as well since it is similarly designed to work on decentralized networks.
- We are seeing blockchain computers, like the early version of the Bitcoin Computer, and blockchain phones built by HTC. These are part of a larger story around how local hardware computing intersects with mesh networks, clouds, and decentralized databases like blockchains to compute and record transactions with data. The work done by devices at the edges is most relevant to the growing Internet of Things – autonomous vehicles or robots that will need real-time data to make decisions or log transactions and which cannot wait for computation to be performed in the cloud and returned with latency.

Information Technology Use Cases for Blockchain (Contd.)

Web 3.0 and Blockchain

- Web 3.0, often referred to as the "semantic web," represents the next evolution of the World Wide Web. While the previous iterations of the web focused on static web pages (Web 1.0) and user-generated content and social networking (Web 2.0), Web 3.0 aims to create a more intelligent, connected, and personalized web experience.
- Here are some key characteristics and concepts associated with Web 3.0:

1. **Semantic Understanding**: Web 3.0 aims to understand and interpret the context of information on the web. Instead of just reading web pages like Web 2.0 does, Web 3.0 aims to understand the meaning behind the content, making the web more intelligent.
2. **Machine Learning and AI**: With advancements in machine learning and artificial intelligence (AI), Web 3.0 can offer more personalized and predictive user experiences. AI can analyze user behavior, preferences, and data to provide tailored recommendations and services.
3. **Decentralization**: Blockchain technology and decentralized protocols play a significant role in Web 3.0. Decentralization aims to shift control from centralized entities to users, enabling more transparency, security, and ownership of data and digital assets.

Information Technology Use Cases for Blockchain (Contd.)

Web 3.0 and Blockchain

4. Interoperability: Web 3.0 aims to create a more interconnected web where different applications and platforms can seamlessly communicate and share data. This interoperability can lead to new innovative services and functionalities.

5. **Personalization**: With the help of AI and semantic understanding, Web 3.0 can offer highly personalized user experiences. Websites and applications can adapt to individual user preferences, making interactions more relevant and engaging.

6.**Smart Contracts**: Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They run on blockchain platforms like Ethereum and enable automated and trustless transactions, reducing the need for intermediaries.

7.**WebAssembly and Decentralized Computing**: WebAssembly (Wasm) allows for high-performance computing in web browsers, enabling more complex and powerful web applications. Decentralized computing platforms also enable distributed processing and storage, supporting the growth of decentralized applications (dApps).

- Overall, Web 3.0 represents a shift towards a more intelligent, decentralized, and user-centric web. It aims to overcome the limitations of previous web iterations by leveraging advanced technologies like AI, blockchain, and decentralized protocols to create a more connected and personalized online experience.

Information Technology Use Cases for Blockchain (Contd.)

Web 3.0 and Blockchain

- Tim Berners-Lee, founder of the World Wide Web has been looking into blockchain as a part of the next iteration of the Internet, or what most are calling Web 3.0.
- If you look back at the origin story of the first World Wide Web, Berners-Lee has said, “In those days, there was different information on different computers, but you had to log on to different computers to get at it.”
- Blockchain is part of the early steps toward Web 3.0 and offers novel ways to create shared realities not just for humans but also for machines.
- Several groups are trying to move the agenda forward in developing a Web 3.0. For instance, the Web3 Foundation advocates for a shift to a server-less Internet, or as their site describes, “An internet where users are in control of their own data, identity and destiny.”

Information Technology Use Cases for Blockchain (Contd.)

Web 3.0 and Blockchain

- Other organizations, like the Internet of Blockchain Foundation based in the Netherlands, are trying to foster the adoption of Web 3.0 through user-friendly decentralized frameworks such as Essentia.one.
- One key aim of Web 3.0 technology is to make encounters opt-in rather than opt-out, and provide greater control for users over their own data as well as digital assets.
- The services that are being built on top of Web 3.0 infrastructure include file distribution and storage (e.g. Storj, Siacoin, Filecoin, IPFS), decentralized versions of communication platforms like Skype (e.g. Experty.io) and social networks that offer micro-transactions instead of Facebook (e.g. Steemit), as well as freelance networks that function like Upwork (e.g. Ethlance).
- There’s even a competitor to the already crowd-sourced dictionary Wikipedia that is blockchain-based, called Everipedia.
- These services are still in their infancy but much of the excitement around blockchain technology lies in its relationship to a greater vision for a decentralized economic infrastructure to underpin our digital world.

Obstacles in Blockchain

1. **Sybil Attacks**

- These are attacks where a peer-to-peer system is subverted when a node in the network forges multiple identities and wields undue influence.
- The main Sybil attack concern in the Bitcoin network is a 51% attack, wherein a majority of the network computing power gets controlled by one actor.
- Proof of Work requires substantial computing resources, making this kind of attack very expensive.
- An attacker would need to pay to control many nodes at the same time and for long enough to alter transaction history.

Obstacles in Blockchain (Contd.)

2. Key Management

- You have likely lost your house keys or your smartphone at some point in your lifetime.
- Imagine losing the keys to your funds and not being able to go to the bank to request a new set.
- This is the problem of managing cryptographic keys for blockchain users: they are highly sensitive and need to be kept safe but are also relatively easy to lose for most people.

Obstacles in Blockchain (Contd.)

3. Scalability

- There have been many arguments made in blockchain’s short lifespan about the problem of scale.
- This argument typically takes shape around whether block size is capable of accommodating all the transactions in the network over time, about the amount of storage and memory needed to download and validate the entire blockchain as it grows, and even about the volume of transaction throughput that is possible.
- Scalability questions remain about replicating applications across every node, and about using PoW consensus which requires large amounts of computing power, and thus consumes real-world energy at a growing rate as the network expands.
- There are many developments underway to tackle different elements of these scalability debates. **Some are focusing on “layer-2 scaling,” or off-chain solutions that move transaction volume off-chain, and use blockchains as a settlement layer.**
- **Other approaches like “sharding” seek to split the entire state of the chain into partitions, or “shards,” that have independent pieces of the state.**

Obstacles in Blockchain (Contd.)

4. Updating and Governance

- There are some concerns for permissionless blockchains in particular over who controls the updating, maintenance, and directional influence of these networks.
- In theory, there are core developers, client developers, miners, and users, who all have checks and balances based on the ability to propose changes openly on forums as well as update or fork their software in response to code changes.
- The Ethereum Foundation, which updates the Ethereum network, has moved to streaming its governance conversations live online in order to improve transparency in how its network is governed.