Blockchain

A blockchain is a distributed ledger with growing lists of records (blocks) that are securely linked together via cryptographic hashes. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves). Since each block contains information about the previous block, they effectively form a chain (compare linked list data structure), with each additional block linking to the ones before it. Consequently, blockchain transactions are resistant to alteration because, once recorded, the data in any given block cannot be changed retroactively without altering all subsequent blocks and obtaining network consensus to accept these changes.

Blockchains are typically managed by a peer-to-peer (P2P) computer network for use as a public distributed ledger, where nodes collectively adhere to a consensus algorithm protocol to add and validate new transaction blocks. Although blockchain records are not unalterable, since blockchain forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance.

A blockchain was created by a person (or group of people) using the name (or pseudonym) Satoshi Nakamoto in 2008 to serve as the public distributed ledger for bitcoin cryptocurrency transactions, based on previous work by Stuart Haber, W. Scott Stornetta, and Dave Bayer. The implementation of the blockchain within bitcoin made it the first digital currency to solve the double-spending problem without the need for a trusted authority or central server. The bitcoin design has inspired other applications and blockchains that are readable by the public and are widely used by cryptocurrencies. The blockchain may be considered a type of payment rail.

Private blockchains have been proposed for business use. Computerworld called the marketing of such privatized blockchains without a proper security model "snake oil"; however, others have argued that permissioned blockchains, if carefully designed, may be more decentralized and therefore more secure in practice than permissionless ones.

History

Cryptographer David Chaum first proposed a blockchain-like protocol in his 1982 dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups". Further work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system wherein document timestamps could not be tampered with. In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle trees into the design, which improved its efficiency by allowing several document certificates to be collected into one block. Under their company Surety, their document certificate hashes have been published in The New York Times every week since 1995.

The first decentralized blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto improved the design in an important way using a Hashcash-like method to timestamp blocks without requiring them to be signed by a trusted party and introducing a difficulty parameter to stabilize the rate at which blocks are added to the chain. The design 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.

In August 2014, the bitcoin blockchain file size, containing records of all transactions that have occurred on the network, reached 20 GB (gigabytes). In January 2015, the size had grown to almost 30 GB, and from January 2016 to January 2017, the bitcoin blockchain grew from 50 GB to 100 GB in size. The ledger size had exceeded 200 GB by early 2020.

The words block and chain were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, blockchain, by 2016.

According to Accenture, an application of the diffusion of innovations theory suggests that blockchains attained a 13.5% adoption rate within financial services in 2016, therefore reaching the early adopters'phase. Industry trade groups joined to create the Global Blockchain Forum in 2016, an initiative of the Chamber of Digital Commerce.

In May 2018, Gartner found that only 1% of CIOs indicated any kind of blockchain adoption within their organisations, and only 8% of CIOs were in the short-term "planning or [looking at] active experimentation with blockchain". For the year 2019 Gartner reported 5% of CIOs believed blockchain technology was a 'game-changer'for their business.

Structure and design

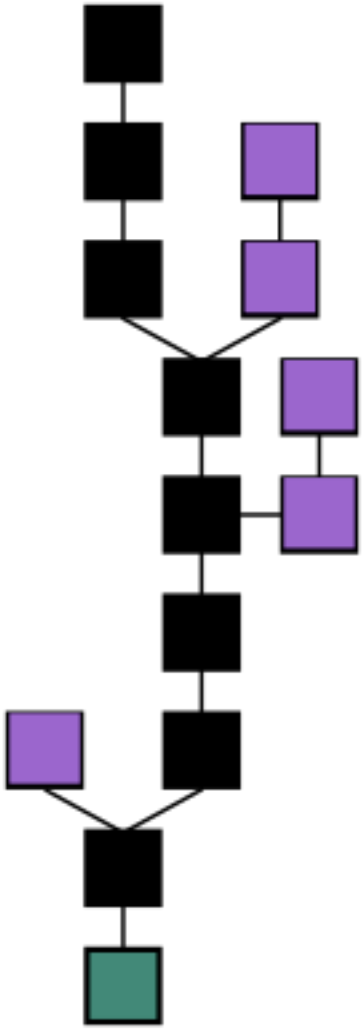

Figure 1: Blockchain formation. The main chain (black) consists of the longest series of blocks from the genesis block (green) to the current block. Orphan blocks (purple) exist outside of the main chain.

A blockchain is a decentralized, distributed, and often public, digital ledger consisting of records called blocks that are used to record transactions across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double-spending. A blockchain has been described as a value-exchange protocol.

Logically, a blockchain can be seen as consisting of several layers:

- infrastructure (hardware)
- networking (node discovery, information propagation and verification)
- consensus (proof of work, proof of stake)
- data (blocks, transactions)
- application (smart contracts/decentralized applications, if applicable)

Blocks

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the initial block, which is known as the genesis block (Block 0). To assure the integrity of a block and the data contained in it, the block is usually digitally signed.

Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher score can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of history forever. Blockchains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks. Therefore, the probability of an entry becoming superseded decreases exponentially as more blocks are built on top of it, eventually becoming very low.: ch. 08 For example, bitcoin uses a proof-of-work system, where the chain with the most cumulative proof-of-work is considered the valid one by the network. There are a number of methods that can be used to demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

The block time is the average time it takes for the network to generate one extra block in the blockchain. By the time of block completion, the included data becomes verifiable. In cryptocurrency, this is practically when the transaction takes place, so a shorter block time means faster transactions. The block time for Ethereum is set to between 14 and 15 seconds, while for bitcoin it is on average 10 minutes.

A hard fork is a change to the blockchain protocol that is not backward compatible and requires all users to upgrade their software in order to continue participating in the network. In a hard fork, the network splits into two separate versions: one that follows the new rules and one that follows the old rules.

For example, Ethereum was hard forked in 2016 to "make whole"the investors in The DAO, which had been hacked by exploiting a vulnerability in its code. In this case, the fork resulted in a split creating Ethereum and Ethereum Classic chains. In 2014, the Nxt community was asked to consider a hard fork that would have led to a rollback of the blockchain records to mitigate the effects of a theft of 50 million NXT from a major cryptocurrency exchange. The hard fork proposal was rejected, and some of the funds were recovered after negotiations and ransom payment. Alternatively, to prevent a permanent split, a majority of nodes using the new software may return to the old rules, as was the case with Bitcoin split on 12 March 2013.

Decentralization

By storing data across its peer-to-peer network, the blockchain eliminates some risks that come with data being held centrally. The decentralized blockchain may use ad hoc message passing and distributed networking.

In a so-called "51% attack"a central entity gains control of more than half of a network and can then manipulate that specific blockchain record at will, allowing double-spending.

Blockchain security methods include the use of public-key cryptography.: 5 A public key (a long, random-looking string of numbers) is an address on the blockchain. Value tokens sent across the network are recorded as belonging to that address. A private key is like a password that gives its owner access to their digital assets or the means to otherwise interact with the various capabilities that blockchains now support. Data stored on the blockchain is generally considered incorruptible.

Every node in a decentralized system has a copy of the blockchain. Data quality is maintained by massive database replication and computational trust. No centralized "official"copy exists and no user is "trusted"more than any other. Transactions are broadcast to the network using the software. Messages are delivered on a best-effort basis. Early blockchains rely on energy-intensive mining nodes to validate transactions, add them to the block they are building, and then broadcast the completed block to other nodes.: ch. 08 Blockchains use various time-stamping schemes, such as proof-of-work, to serialize changes. Later consensus methods include proof of stake. The growth of a decentralized blockchain is accompanied by the risk of centralization because the computer resources required to process larger amounts of data become more expensive.

Finality is the level of confidence that the well-formed block recently appended to the blockchain will not be revoked in the future (is "finalized") and thus can be trusted. Most distributed blockchain protocols, whether proof of work or proof of stake, cannot guarantee the finality of a freshly committed block, and instead rely on "probabilistic finality": as the block goes deeper into a blockchain, it is less likely to be altered or reverted by a newly found consensus.

Byzantine fault tolerance-based proof-of-stake protocols purport to provide so called "absolute finality": a randomly chosen validator proposes a block, the rest of validators vote on it, and, if a supermajority decision approves it, the block is irreversibly committed into the blockchain. A modification of this method, an "economic finality", is used in practical protocols, like the Casper protocol used in Ethereum: validators which sign two different blocks at the same position in the blockchain are subject to "slashing", where their leveraged stake is forfeited.

Openness

Open blockchains are more user-friendly than some traditional ownership records, which, while open to the public, still require physical access to view. Because all early blockchains were permissionless, controversy has arisen over the blockchain definition. An issue in this ongoing debate is whether a private system with verifiers tasked and authorized (permissioned) by a central authority should be considered a blockchain. Proponents of permissioned or private chains argue that the term "blockchain"may be applied to any data structure that batches data into time-stamped blocks. These blockchains serve as a distributed version of multiversion concurrency control (MVCC) in databases. Just as MVCC prevents two transactions from concurrently modifying a single object in a database, blockchains prevent two transactions from spending the same single output in a blockchain.: 30–31 Opponents say that permissioned systems resemble traditional corporate databases, not supporting decentralized data verification, and that such systems are not hardened against operator tampering and revision. Nikolai Hampton of Computerworld said that "many in-house blockchain solutions will be nothing more than cumbersome databases,"and "without a clear security model, proprietary blockchains should be eyed with suspicion."

An advantage to an open, permissionless, or public, blockchain network is that guarding against bad actors is not required and no access control is needed. This means that applications can be added to the network without the approval or trust of others, using the blockchain as a transport layer.

Bitcoin and other cryptocurrencies currently secure their blockchain by requiring new entries to include proof of work. To prolong the blockchain, bitcoin uses Hashcash puzzles. While Hashcash was designed in 1997 by Adam Back, the original idea was first proposed by Cynthia Dwork and Moni Naor and Eli Ponyatovski in their 1992 paper "Pricing via Processing or Combatting Junk Mail".

In 2016, venture capital investment for blockchain-related projects was weakening in the US but increasing in China. Bitcoin and many other cryptocurrencies use open (public) blockchains. As of April 2018[update], bitcoin has the highest market capitalization.

Permissioned blockchains use an access control layer to govern who has access to the network. It has been

argued that permissioned blockchains can guarantee a certain level of decentralization, if carefully designed, as opposed to permissionless blockchains, which are often centralized in practice.

Nikolai Hampton argued in Computerworld that "There is also no need for a '51 percent'attack on a private blockchain, as the private blockchain (most likely) already controls 100 percent of all block creation resources. If you could attack or damage the blockchain creation tools on a private corporate server, you could effectively control 100 percent of their network and alter transactions however you wished."This has a set of particularly profound adverse implications during a financial crisis or debt crisis such as the 2008 financial crisis, where politically powerful actors may make decisions that favor some groups at the expense of others, and "the bitcoin blockchain is protected by the massive group mining effort. It's unlikely that any private blockchain will try to protect records using gigawatts of computing power —it's time-consuming and expensive."He also said, "Within a private blockchain there is also no 'race'; there's no incentive to use more power or discover blocks faster than competitors. This means that many in-house blockchain solutions will be nothing more than cumbersome databases."

The analysis of public blockchains has become increasingly important with the popularity of bitcoin, Ethereum, litecoin and other cryptocurrencies. A blockchain, if it is public, provides access to anyone to observe and analyse the chain data, given the know-how. The process of understanding and accessing the flow of crypto has been an issue for many cryptocurrencies, crypto exchanges and banks. The reason for this is accusations of blockchain-enabled cryptocurrencies enabling illicit dark market trading of drugs, weapons, money laundering, etc. A common belief has been that cryptocurrency is private and untraceable, thus leading many actors to use it for illegal purposes. This is changing now that specialised tech companies provide blockchain tracking services, making crypto exchanges, law-enforcement and banks more aware of what is happening with crypto funds and fiat-crypto exchanges. The development, some argue, has led criminals to prioritise the use of new cryptos such as Monero.

Standardisation

In April 2016, Standards Australia submitted a proposal to the International Organization for Standardization to consider developing standards to support blockchain technology. This proposal resulted in the creation of ISO Technical Committee 307, Blockchain and Distributed Ledger Technologies. The technical committee has working groups relating to blockchain terminology, reference architecture, security and privacy, identity, smart contracts, governance and interoperability for blockchain and DLT, as well as standards specific to industry sectors and generic government requirements.[non-primary source needed] More than 50 countries are participating in the standardization process together with external liaisons such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the European Commission, the International Federation of Surveyors, the International Telecommunication Union (ITU) and the United Nations Economic Commission for Europe (UNECE).

Many other national standards bodies and open standards bodies are also working on blockchain standards. These include the National Institute of Standards and Technology (NIST), the European Committee for Electrotechnical Standardization (CENELEC), the Institute of Electrical and Electronics Engineers (IEEE), the Organization for the Advancement of Structured Information Standards (OASIS), and some individual participants in the Internet Engineering Task Force (IETF).

Centralized blockchain

Although most of blockchain implementation are decentralized and distributed, Oracle launched a centralized blockchain table feature in Oracle 21c database. The Blockchain Table in Oracle 21c database is a centralized blockchain which provide immutable feature. Compared to decentralized blockchains, centralized blockchains normally can provide a higher throughput and lower latency of transactions than consensus-based distributed blockchains.

Types

Currently, there are at least four types of blockchain networks —public blockchains, private blockchains, consortium blockchains and hybrid blockchains.

Public blockchains

A public blockchain has no access restrictions. Anyone with an Internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol).‹The template Self-published inline is being considered for merging.› [self-published source?] Usually, such networks offer economic incentives for those who secure them and utilize some type of a proof-of-stake or proof-of-work algorithm.

Some of the largest, most known public blockchains are the bitcoin blockchain and the Ethereum blockchain.

Private blockchains

A private blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted. To distinguish between open blockchains and other peer-to-peer decentralized database applications that are not open ad-hoc compute clusters, the terminology Distributed Ledger (DLT) is normally used for private blockchains.

Hybrid blockchains

A hybrid blockchain has a combination of centralized and decentralized features. The exact workings of the chain can vary based on which portions of centralization and decentralization are used.

Sidechains

A sidechain is a designation for a blockchain ledger that runs in parallel to a primary blockchain. Entries from the primary blockchain (where said entries typically represent digital assets) can be linked to and from the sidechain; this allows the sidechain to otherwise operate independently of the primary blockchain (e.g., by using an alternate means of record keeping, alternate consensus algorithm, etc.).[better source needed]

Consortium blockchain

A consortium blockchain is a type of blockchain that combines elements of both public and private blockchains. In a consortium blockchain, a group of organizations come together to create and operate the blockchain, rather than a single entity. The consortium members jointly manage the blockchain network and are responsible for validating transactions. Consortium blockchains are permissioned, meaning that only certain individuals or organizations are allowed to participate in the network. This allows for greater control over who can access the blockchain and helps to ensure that sensitive information is kept confidential.

Consortium blockchains are commonly used in industries where multiple organizations need to collaborate on a common goal, such as supply chain management or financial services. One advantage of consortium blockchains is that they can be more efficient and scalable than public blockchains, as the number of nodes required to validate transactions is typically smaller. Additionally, consortium blockchains can provide greater security and reliability than private blockchains, as the consortium members work together to maintain the network. Some examples of consortium blockchains include Quorum and Hyperledger.

Uses

Blockchain technology can be integrated into multiple areas. The primary use of blockchains is as a distributed ledger for cryptocurrencies such as bitcoin; there were also a few other operational products that had matured from proof of concept by late 2016. As of 2016, some businesses have been testing the technology and conducting low-level implementation to gauge blockchain's effects on organizational efficiency in their back office.

Blockchain is seen as a pivotal technological advancement of the 21st century, with the ability to impact organizations at strategic, operational, and market levels. In 2019, it was estimated that around $2.9 billion were invested in blockchain technology, which represents an 89% increase from the year prior. Additionally, the International Data Corp estimated that corporate investment into blockchain technology would reach $12.4 billion by 2022. Furthermore, According to PricewaterhouseCoopers (PwC), the second-largest professional services network in the world, blockchain technology has the potential to generate an annual business value of more than $3 trillion by 2030. PwC's estimate is further augmented by a 2018 study that they have conducted, in which PwC surveyed 600 business executives and determined that 84% have at least some exposure to utilizing blockchain technology, which indicates a significant demand and interest in blockchain technology.

In 2019, the BBC World Service radio and podcast series Fifty Things That Made the Modern Economy identified blockchain as a technology that would have far-reaching consequences for economics and society. The economist and Financial Times journalist and broadcaster Tim Harford discussed why the underlying technology might have much wider applications and the challenges that needed to be overcome. His first broadcast was on 29 June 2019.

The number of blockchain wallets quadrupled to 40 million between 2016 and 2020.

A paper published in 2022 discussed the potential use of blockchain technology in sustainable management.

Cryptocurrencies

Most cryptocurrencies are designed to gradually decrease the production of that currency, placing a cap on the total amount of that currency that will ever be in circulation. Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies can be more difficult for seizure by law enforcement.

The validity of each cryptocurrency's coins is provided by a blockchain. A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain.

In the context of cryptocurrencies, the blockchain serves as a public ledger for all transactions. Cryptocurrencies use various timestamping schemes to "prove the validity of transactions added to the blockchain ledger without the need for a trusted third party".

The first cryptocurrency was Bitcoin, which was first released as open-source software in 2009.

As cryptocurrencies have gained prominence, several countries have made advancements in their private and commercial law treatment to address legal uncertainties. In the United States, for example, the 2022 amendments to the Uniform Commercial Code (UCC) introduced Article 12, which establishes "controllable electronic records"(CERs) as a new category of personal property. This framework provides legal clarity for the ownership, transfer, and use of cryptocurrencies as CERs, with the concept of "control"serving as a functional equivalent to possession for digital assets. These reforms aim to align legal standards with market practices, reducing title disputes and supporting the integration of cryptocurrencies into commercial transactions.

Smart contracts

Blockchain-based smart contracts are contracts that can be partially or fully executed or enforced without human interaction. One of the main objectives of a smart contract is automated escrow. A key feature of smart contracts is that they do not need a trusted third party (such as a trustee) to act as an intermediary between contracting entities —the blockchain network executes the contract on its own. This may reduce friction between entities when transferring value and could subsequently open the door to a higher level of transaction automation. An IMF staff discussion from 2018 reported that smart contracts based on blockchain technology might reduce moral hazards and optimize the use of contracts in general, but "no viable smart contract systems have yet emerged."Due to the lack of widespread use, their legal status was unclear.

Financial services

According to Reason, many banks have expressed interest in implementing distributed ledgers for use in banking and are cooperating with companies creating private blockchains; according to a September 2016 IBM study, it is occurring faster than expected. It has been estimated by the World Economic Forum that by 2025, 10% of the world's GDP will be stored on blockchain related technology.

Banks are interested in this technology not least because it has the potential to speed up back office settlement systems. Moreover, as the blockchain industry has reached early maturity institutional appreciation has grown that it is, practically speaking, the infrastructure of a whole new financial industry, with all the implications which that entails. This technology will transform financial transactions due to its ability to enhance data storage, process simultaneous transactions, lessen transaction costs, and improve capital market transparency for debt and equity capital administration.

Banks such as UBS are opening new research labs dedicated to blockchain technology in order to explore how blockchain can be used in financial services to increase efficiency and reduce costs.

Berenberg, a German bank, believes that blockchain is an "overhyped technology"that has had a large number of "proofs of concept", but still has major challenges, and very few success stories.

The blockchain has also given rise to initial coin offerings (ICOs) as well as a new category of digital asset called security token offerings (STOs), also sometimes referred to as digital security offerings (DSOs). STO/DSOs may be conducted privately or on public, regulated stock exchange and are used to tokenize traditional assets such as company shares as well as more innovative ones like intellectual property, real estate, art, or individual products. A number of companies are active in this space providing services for compliant tokenization, private STOs, and public STOs.

Games

Blockchain technology, such as cryptocurrencies and non-fungible tokens (NFTs), has been used in video games for monetization. Many live-service games offer in-game customization options, such as character skins or other in-game items, which the players can earn and trade with other players using in-game currency. Some games also allow for trading of virtual items using real-world currency, but this may be illegal in some countries where video games are seen as akin to gambling, and has led to gray market issues such as skin gambling, and thus publishers typically have shied away from allowing players to earn real-world funds from games. Blockchain games typically allow players to trade these in-game items for cryptocurrency, which can then be exchanged for money.

The first known game to use blockchain technologies was CryptoKitties, launched in November 2017, where the player would purchase NFTs with Ethereum cryptocurrency, each NFT consisting of a virtual pet that the player could breed with others to create offspring with combined traits as new NFTs. The game made headlines in December 2017 when one virtual pet sold for more than US$100,000. CryptoKitties also illustrated scalability problems for games on Ethereum when it created significant congestion on the Ethereum network in early 2018 with approximately 30% of all Ethereum transactions[clarification needed] being for the game.

By the early 2020s, there had not been a breakout success in video games using blockchain, as these games tend to focus on using blockchain for speculation instead of more traditional forms of gameplay, which offers limited appeal to most players. Such games also represent a high risk to investors as their revenues can be difficult to predict. However, limited successes of some games, such as Axie Infinity during the COVID-19 pandemic, and corporate plans towards metaverse content, refueled interest in the area of GameFi, a term describing the intersection of video games and financing typically backed by blockchain currency, in the second half of 2021. Several major publishers, including Ubisoft, Electronic Arts, and Take Two Interactive, have stated that blockchain and NFT-based games are under serious consideration for their companies in the future.

In October 2021, Valve Corporation banned blockchain games, including those using cryptocurrency and NFTs, from being hosted on its Steam digital storefront service, which is widely used for personal computer gaming, claiming that this was an extension of their policy banning games that offered in-game items with real-world value. Valve's prior history with gambling, specifically skin gambling, was speculated to be a factor in the decision to ban blockchain games. Journalists and players responded positively to Valve's decision as blockchain and NFT games have a reputation for scams and fraud among most PC gamers, and Epic Games, which runs the Epic Games Store in competition to Steam, said that they would be open to accepted blockchain games in the wake of Valve's refusal.

Supply chain

There have been several different efforts to employ blockchains in supply chain management.

- Precious commodities mining —Blockchain technology has been used for tracking the origins of gemstones and other precious commodities. In 2016, The Wall Street Journal reported that the blockchain technology company Everledger was partnering with IBM's blockchain-based tracking service to trace the origin of diamonds to ensure that they were ethically mined. As of 2019, the Diamond Trading Company (DTC) has been involved in building a diamond trading supply chain product called Tracer.
- Food supply —As of 2018, Walmart and IBM were running a trial to use a blockchain-backed system for supply chain monitoring for lettuce and spinach –all nodes of the blockchain were administered by Walmart and located on the IBM cloud.
- Fashion industry —There is an opaque relationship between brands, distributors, and customers in the fashion industry, which prevents the sustainable and stable development of the fashion industry. Blockchain could make this information transparent, assisting sustainable development of the industry.
- Motor vehicles —Mercedes-Benz and partner Icertis developed a blockchain prototype used to facilitate consistent documentation of contracts along the supply chain so that the ethical standards and contractual obligations required of its direct suppliers can be passed on to second tier suppliers and beyond. In another project, the company uses blockchain technology to track the emissions of climate-relevant gases and the amount of secondary material along the supply chain for its battery cell manufacturers.

Domain names

There are several different efforts to offer domain name services via the blockchain. These domain names can be controlled by the use of a private key, which purports to allow for uncensorable websites. This would also bypass a registrar's ability to suppress domains used for fraud, abuse, or illegal content.

Namecoin is a cryptocurrency that supports the ".bit"top-level domain (TLD). Namecoin was forked from bitcoin in 2011. The .bit TLD is not sanctioned by ICANN, instead requiring an alternative DNS root. As of 2015, .bit was used by 28 websites, out of 120,000 registered names. Namecoin was dropped by OpenNIC in 2019, due to malware and potential other legal issues. Other blockchain alternatives to ICANN include The Handshake Network, EmerDNS, and Unstoppable Domains.

Specific TLDs include ".eth", ".luxe", and ".kred", which are associated with the Ethereum blockchain through the Ethereum Name Service (ENS). The .kred TLD also acts as an alternative to conventional cryptocurrency wallet addresses as a convenience for transferring cryptocurrency.

Other uses

Blockchain technology can be used to create a permanent, public, transparent ledger system for compiling data on sales, tracking digital use and payments to content creators, such as wireless users or musicians. The Gartner 2019 CIO Survey reported 2% of higher education respondents had launched blockchain projects and another 18% were planning academic projects in the next 24 months. In 2017, IBM partnered with ASCAP and PRS for Music to adopt blockchain technology in music distribution. Imogen Heap's Mycelia service has also been proposed as a blockchain-based alternative "that gives artists more control over how their songs and associated data circulate among fans and other musicians."

New distribution methods are available for the insurance industry such as peer-to-peer insurance, parametric insurance and microinsurance following the adoption of blockchain. The sharing economy and IoT are also set to benefit from blockchains because they involve many collaborating peers. The use of blockchain in libraries is being studied with a grant from the U.S. Institute of Museum and Library Services.

Other blockchain designs include Hyperledger, a collaborative effort from the Linux Foundation to support blockchain-based distributed ledgers, with projects under this initiative including Hyperledger Burrow (by Monax) and Hyperledger Fabric (spearheaded by IBM). Another is Quorum, a permissioned private blockchain by JPMorgan Chase with private storage, used for contract applications.

Oracle introduced a blockchain table feature in its Oracle 21c database.

Blockchain is also being used in peer-to-peer energy trading.

Lightweight blockchains, or simplified blockchains, are more suitable for internet of things (IoT) applications than conventional blockchains. One experiment suggested that a lightweight blockchain-based network could accommodate up to 1.34 million authentication processes every second, which could be sufficient for resource-constrained IoT networks.

Blockchain could be used in detecting counterfeits by associating unique identifiers to products, documents and shipments, and storing records associated with transactions that cannot be forged or altered. It is however argued that blockchain technology needs to be supplemented with technologies that provide a strong binding between physical objects and blockchain systems, as well as provisions for content creator verification ala KYC standards. The EUIPO established an Anti-Counterfeiting Blockathon Forum, with the objective of "defining, piloting and implementing"an anti-counterfeiting infrastructure at the European level. The Dutch Standardisation organisation NEN uses blockchain together with QR Codes to authenticate certificates.

Beijing and Shanghai are among the cities designated by China to trial blockchain applications as January 30, 2022. In Chinese legal proceedings, blockchain technology was first accepted as a method for authenticating internet evidence by the Hangzhou Internet Court in 2019 and has since been accepted by other Chinese courts.: 123–125

Blockchain interoperability

With the increasing number of blockchain systems appearing, even only those that support cryptocurrencies, blockchain interoperability is becoming a topic of major importance. The objective is to support transferring assets from one blockchain system to another blockchain system. Wegner stated that "interoperability is the ability of two or more software components to cooperate despite differences in language, interface, and execution platform". The objective of blockchain interoperability is therefore to support such cooperation among blockchain systems, despite those kinds of differences.

There are already several blockchain interoperability solutions available. They can be classified into three categories: cryptocurrency interoperability approaches, blockchain engines, and blockchain connectors.

Several individual IETF participants produced the draft of a blockchain interoperability architecture.

Energy consumption concerns

Some cryptocurrencies use blockchain mining, namely the peer-to-peer computer computations by which transactions are validated and verified. This requires a large amount of energy. In June 2018, the Bank for International Settlements criticized the use of public proof-of-work blockchains for their high energy consumption.

Early concern over the high energy consumption was a factor in later blockchains such as Cardano (2017), Solana (2020) and Polkadot (2020) adopting the less energy-intensive proof-of-stake model. Researchers have estimated that bitcoin consumes 100,000 times as much energy as proof-of-stake networks.

In 2021, a study by Cambridge University determined that bitcoin (at 121 terawatt-hours per year) used more electricity than Argentina (at 121TWh) and the Netherlands (109TWh). According to Digiconomist, one bitcoin transaction required 708 kilowatt-hours of electrical energy, the amount an average U.S. household consumed in 24 days.

In February 2021, U.S. Treasury secretary Janet Yellen called bitcoin "an extremely inefficient way to conduct transactions", saying "the amount of energy consumed in processing those transactions is staggering". In March 2021, Bill Gates stated that "Bitcoin uses more electricity per transaction than any other method known to mankind", adding "It's not a great climate thing."

Nicholas Weaver, of the International Computer Science Institute at the University of California, Berkeley, examined blockchain's online security, and the energy efficiency of proof-of-work public blockchains, and in both cases found it grossly inadequate. The 31TWh-45TWh of electricity used for bitcoin in 2018 produced 17–23 million tonnes of CO2. By 2022, the University of Cambridge and Digiconomist estimated that the two largest proof-of-work blockchains, bitcoin and Ethereum, together used twice as much electricity in one year as the whole of Sweden, leading to the release of up to 120 million tonnes of CO2 each year.

Some cryptocurrency developers are considering moving from the proof-of-work model to the proof-of-stake model. In Sept, 2022, Ethereum converted from proof-of-work to proof-of-stake.

Academic research

Figure 2: Blockchain panel discussion at the first IEEE Computer Society TechIgnite conference

In October 2014, the MIT Bitcoin Club, with funding from MIT alumni, provided undergraduate students at the Massachusetts Institute of Technology access to $100 of bitcoin. The adoption rates, as studied by Catalini and Tucker (2016), revealed that when people who typically adopt technologies early are given delayed access, they tend to reject the technology. Many universities have founded departments focusing on crypto and blockchain, including MIT, in 2017. In the same year, Edinburgh became "one of the first big European universities to launch a blockchain course", according to the Financial Times.

Adoption decision

Motivations for adopting blockchain technology (an aspect of innovation adoption) have been investigated by researchers. For example, Janssen, et al. provided a framework for analysis, and Koens & Poll pointed out that adoption could be heavily driven by non-technical factors. Based on behavioral models, Li has discussed the differences between adoption at the individual level and organizational levels.

Collaboration

Scholars in business and management have started studying the role of blockchains to support collaboration. It has been argued that blockchains can foster both cooperation (i.e., prevention of opportunistic behavior) and coordination (i.e., communication and information sharing). Thanks to reliability, transparency, traceability of records, and information immutability, blockchains facilitate collaboration in a way that differs both from the traditional use of contracts and from relational norms. Contrary to contracts, blockchains do not directly rely on the legal system to enforce agreements. In addition, contrary to the use of relational norms, blockchains do not require a trust or direct connections between collaborators.

Blockchain and internal audit

The need for internal audits to provide effective oversight of organizational efficiency will require a change in the way that information is accessed in new formats. Blockchain adoption requires a framework to identify the risk of exposure associated with transactions using blockchain. The Institute of Internal Auditors has identified the need for internal auditors to address this transformational technology. New methods are required to develop audit plans that identify threats and risks. The Internal Audit Foundation study, Blockchain and Internal Audit, assesses these factors. The American Institute of Certified Public Accountants has outlined new roles for auditors as a result of blockchain.

Testnet

In blockchain technology, a testnet is an instance of a blockchain powered by the same or a newer version of the underlying software, to be used for testing and experimentation without risk to real funds or the main chain. Testnet coins are separate and distinct from the official mainnet coins, don't have value, and can be obtained freely from faucets.

Testnets allow for the development of blockchain applications without the risk of losing funds.

Using testnets, a bug was discovered in the Bitcoin Core software that gave miners the ability to take down essential parts of the Bitcoin infrastructure (nodes) by sending a 'bad'block to the blockchain.

Mainnet

A mainnet (short for main network) is the fully operational version of a blockchain where real transactions occur, as opposed to a testnet. It is secured through consensus mechanisms like Proof of Work or Proof of Stake and supports smart contracts, token transfers, and decentralized applications.

A mainnet launch marks the transition from a testnet to a live blockchain, involving security audits, network deployment, and token migration.

Journals

In September 2015, the first peer-reviewed academic journal dedicated to cryptocurrency and blockchain technology research, Ledger, was announced. The inaugural issue was published in December 2016. The journal covers aspects of mathematics, computer science, engineering, law, economics and philosophy that relate to cryptocurrencies. The journal encourages authors to digitally sign a file hash of submitted papers, which are then timestamped into the bitcoin blockchain. Authors are also asked to include a personal bitcoin address on the first page of their papers for non-repudiation purposes.