API-economie
Blockchain & IDS

Table of contents

1 Introduction: What is blockchain?

Ledgers are the system of record for recording asset transfers in and out of a business. Ledgers are nothing new and have been in use since the 13th century for bookkeeping. Assets are anything owned or controlled to produce value. There are two types of assets: tangible (e.g. a house) and intangible (e.g. a mortgage). In today's (business) networks, each participant keeps track of their assets in their own ledger(s), which are updated to represent business transactions as they occur. This is expensive and time consuming due to duplication and effort of intermediaries. It is clearly inefficient, as the business conditions for transactions to occur ('the contract') is duplicated by each network participant. This kind of system is also vulnerable because if a central system (e.g. a bank) is compromised, because of an incident like fraud or cyber-attack, this affects the whole business network.

Enter blockchain. 'Blockchain is a shared, immutable ledger for recording transactions, tracking assets and building trust' – IBM. 'Blockchain is an encrypted digital database shared by several parties in a distributed network, impossible to change or hack' –

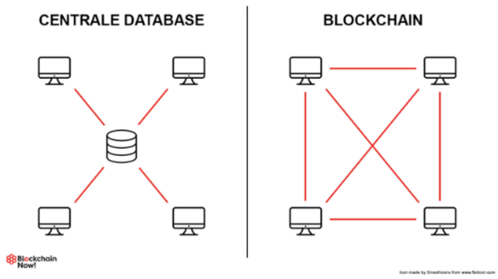
Blockchain is a type of shared, distributed ledger, comprised of digital records containing transactions of assets, accessible to and trusted by all participants running the same protocol. Each transaction in the system is time stamped and verified by a consensus mechanism. The fundamental innovation of blockchain is that it creates a means of establishing and maintaining consensus among the participants in a transaction without the need for either an established trust relationship or a central intermediary. Blockchain technology enables multiple parties in a value chain to efficiently work together based on a single source of truth. It allows people and organisations who may not know each other to collectively agree and permanently record information without a third-part authority. This facilitates sharing data between multiple parties, transferring value in a digital way and eliminating the need for costly reconciliations. By creating trust in sharing data in ways that were not possible before, blockchain has the potential to revolutionise how we share information and carry out transactions online.

JPMorgan.

It's been said that blockchain can do for transactions what the Internet did for information. Just as the Internet upended how we share information, blockchain is a technology that has the potential to revolutionise the way we exchange value, transfer ownership and verify transactions. Anything from currencies to land titles to votes can be tokenized, stored, and exchanged on a blockchain network. Practically anything of value can be tracked and traded on a blockchain network, lowering risk and increasing efficiency. The first manifestation of blockchain technology emerged in 2009 with the Bitcoin blockchain, the first decentralized digital currency. Bitcoin is created, distributed, traded and stored using a decentralized ledger (blockchain). It's a secure, censorship-resistant, peer to peer electronic cash system. Bitcoin and blockchain are not the same. Think of blockchain as an operating system, such as MS Windows or MacOS, and bitcoin as only one of the many applications that can run on that operating system.
Apart of the secure transfer of value, blockchain technology offers a single version of the truth (a permanent forensic record of transactions) and a network state that is completely transparent and exhibited in real time for the benefit of all participants. So blockchain allows increased trust and efficiency in the exchange of almost anything. Additionally, cryptography is used to ensure that transactions are secure, authenticated and verifiable.

- Foolproof distributed, decentralized database that securely sends information and transactions
  ≠ Normal database (central authority has control over the server and database)

  → blockchain is stored on multiple private computers (or nodes, see later) connected to a network that can solve computational enigmas to ensure the network is secure.



- = Decentralized database → no central authority

  → unhackable

Blockchain technologies enable eliminating inefficiencies in B2B processes created by lack of trust and transparency, and create innovative business processes by streamlining the exchange of value along the business network. Blockchain supports a new generation of transactional applications and streamlined business processes by establishing the trust, accountability, and transparency that are essential to smart connected operations.

2 How blockchain works

What's in a name

The name 'blockchain' refers to how transaction data is stored in blocks that are linked together to form a chain. A blockchain is a digital ledger where encrypted blocks containing digital asset data are stored and chained together to create a chronological single source of truth for the data. As the amount of transactions increases, the blockchain gets bigger and bigger. Transactions are logged in the blockchain within a network under the control by rules decided upon by the network participants. The blocks record and confirm the exact time and order of these transactions (see 2.2).

All transactions within a blockchain network are logged on all 'copies' of the blockchain linked to the network. (Digital assets itself are distributed, not copied of transferred.) Transactions are similar to rows you add to an excel spreadsheet, but they're added to the record by blocks. As each transaction occurs, it is recorded as a "block" of data. Those transactions show the movement of an asset that can be tangible (a product) or intangible (intellectual). The data block can record the information of your choice: who, what, when, where, how much and even the condition — such as the temperature of a food shipment.

– IBM (https://www.ibm.com/topics/what-is-blockchain)

Blocks

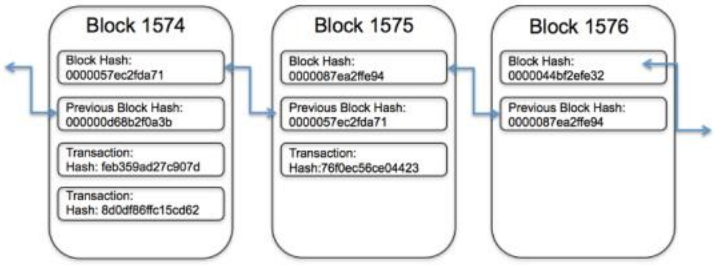
Each (group of) transaction(s) creates a time-stamped "block", and each block is connected to the previous blocks and the ones after it through the digital footprint (see below), forming a chain of data. To prevent any block from being changed or from being added between two already existing blocks, the blocks are securely linked together.

Each block has three certain characteristics:

- A unique digital footprint (cryptographic hash/ block hash) that corresponds with the data in the block
- Timestamped batches of recent valid transactions, data
- The hash of the previous block

A hash is like a fingerprint (long record consisting of some digits and letters, see picture below) that identifies a block. Each block hash is generated with the help of a cryptographic hash algorithm. Consequently, this helps to identify each block in a blockchain structure easily. The moment a block is created, it automatically attaches a hash, while any changes made in a block result in the change of a hash too. Simply stated, hashes help to detect any changes in blocks.

The data stored inside each block depends on the type of blockchain. For instance, in the Bitcoin blockchain structure, the block maintains data about the receiver, sender, and the amount of transacted coins.

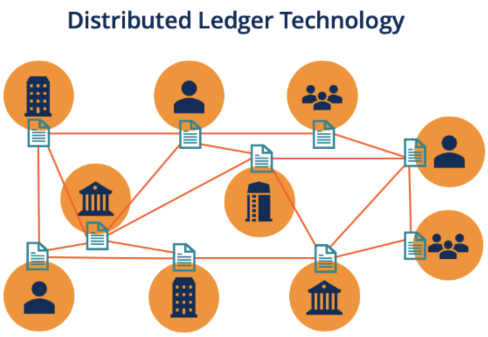


The hash of the previous blocks connects the blocks together and stops any block from being changed or a block being introduced between two already existing blocks. This strengthens the previous block's verification, and ultimately the blockchain as a whole, with each new block that is added. The very first block in a chain is a bit special - all confirmed and validated blocks are derived from this genesis block. This method renders the blockchain tamper-evident, delivering the key strength of immutability. Imagine someone trying to change the content of the fourth block in a chain. While doing this, this person also changes the hash of this fourth block. The fifth block in the chain is still referencing the fourth block by its hash value but the hash value of the fourth block is not valid anymore; it has a new value and therefore the reference is not right anymore, the fifth block is pointing to nowhere. As a result we don't have a blockchain that was existing before, the fourth block was cut off, because the fifth block doesn't have the reference anymore to the fourth block. And because every block is related to its neighbours, the first, second and third block also got cut off. It's very unlikely, but it is possible to also change the hash of the fourth block, the block would have to be "re-mined". But that means that the fifth, sixth, seventh, etc. would also have to be re-mined. Blockchains can easily consist of millions of blocks, making this virtually impossible. Suppose some supercomputer does manage to change the contents and hashes of all the blocks and make a different version of the blockchain by doing so, even then this blockchain is faulty and therefore inoperable. As mentioned earlier, every computer/peer on the network has an identical copy of the blockchain. Now if one particular copy of the blockchain differs from the other copies, then the other peers easily know that something has gone wrong in this "copy" of the blockchain and is therefore invalid. This can be easily checked by looking at the last hash in a blockchain, because every hash needs to be changed to create a different and faulty version of the blockchain. If the hash of the last block in a specific copy of the blockchain differs from the last hashes in all the other copies of the chain this specific copy gets rejected by the other peers in the network.

This is why a blockchain is immutable, first of all, if the content changes, the connections get broken. Second, the blockchain is distributed throughout the whole network. If in one copy the hashes of the blocks don't match with the hashes of the blocks in the other copies of the chain, the other computers know this and make this copy of the blockchain invalid. This removes the possibility of tampering by a malicious actor – and builds a ledger of transactions you and other network members can trust. Any corrupt attempts provoke the blocks to change. All the following blocks then carry incorrect information and render the whole blockchain system invalid.

Transactions are blocked together in an irreversible chain: a blockchain.

Distributed Ledger Technology



To recap: blockchain, also known as Distributed Ledger Technology (DLT), uses decentralization and cryptographic hashing to make the history of any digital asset unchangeable and transparent. DLT is a consensus of geographically dispersed digital data that is copied, shared, and synchronized across multiple sites, countries or institutions, without a central administrator.

An easy comparison to comprehend blockchain technology is a Google Doc. A document is distributed when it is created and shared with a group of individuals, instead of being copied or transferred. This establishes a decentralized chain of distribution that provides simultaneous access to the document for all users. All changes to the document are logged in real-time, making them entirely transparent, and no one is locked out while waiting for updates from another user.

Blockchains can be divided into three types:

- Public (permissionless) - Public blockchains are the foundation of the majority of cryptocurrencies, like bitcoin. Public blockchains usually cost more to operate and do not have the speed seen with consortium or private blockchains. However, they offer better transparency than the others and let anyone connect to the network. Because Bitcoin is accessible to anyone, it is an example of an open, or a permissionless blockchain.
- Private (permissioned) - Private blockchains limit who can access and write additional information to the chain. Private companies tend to use this option because they can control the features and modify it for various reasons. Optimal for business.

- Consortium – Consortium blockchain platforms have many of the same advantages of a private blockchain, but operate under the leadership of a group of businesses instead of a single entity.

Blockchain architecture

Below the core blockchain architecture components are listed:

- Node – User or computer within the blockchain network that runs the blockchain's software to validate and store the complete history of transactions on the network (each has an independent 'copy' of the whole ledger).
- Transaction – The smallest component of a blockchain system (records, information…) that fulfils the function of blockchain
- Block – A data structure that is used to store a set of transactions that are dispersed to all network nodes (see 2.2).
  Each new user (node) joining the peer-to-peer network of the blockchain receives a full copy of the blockchain. Once a new block is created, it is sent to each node within the blockchain system. Then, each node verifies the block and checks whether the information stated there is correct. If everything is alright, the block is added to the local blockchain in each node.
- Chain – A sequence of blocks in a particular order.
- Consensus (consensus protocol) – A set of network rules and arrangements to carry out blockchain operations (Bitcoin for example uses Proof of Work).

Every new transaction within the blockchain implies the creation of a new block. The authenticity of each record is then confirmed and digitally signed. This block should be validated by the majority (>50%) of system nodes before being added to the network.

To recap, all this makes blockchain technology immutable and cryptographically secure by eliminating any third-parties. It is impossible to tamper with the blockchain system; as it would be necessary to tamper with all of its blocks, recalculate the proof-of-work for each block, and also control more than 50% of all the nodes in a peer-to-peer network.

Key elements of a blockchain

The above mentioned blockchain architecture ensures the blockchain has three key elements:

- Distributed ledger technology:
  All network participants/nodes have access to the blockchain and its immutable record of transactions. This shared ledger makes sure transactions are recorded only once, eliminating the duplication of effort that's typical of conventional business networks. The system of record, one single source of truth.

- Immutable records:
  Once a transaction has been added to the blockchain, no participant can alter it or interfere with it. A new transaction must be added to undo an error in a transaction, both transactions are then visible.

- Smart contracts:

A set of rules, also called a smart contract, can be stored on the blockchain to speed up transactions and execute them automatically.

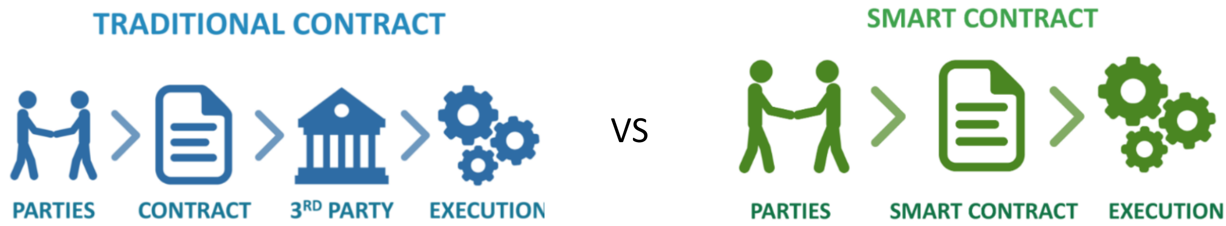
Smart contracts

Smart contracts are different from traditional contracts in two ways:

- Not necessarily legally binding (yet)
- Smart contracts carry out peer-to-peer agreements that conclude on their own when everything in the contract is completed.

A smart contract is an agreement or set of rules that govern a business transaction; it's stored on the blockchain and is executed automatically as a part of a transaction, when certain conditions and predefined terms are met.

Smart contracts can be easily understood by comparing them to vending machines. It takes some time for a vending machine to offer you a soda can once you insert a coin and press the soda button. Similar to this, smart contracts are short programs that carry out "if this happens then do that" instructions on the blockchain and are validated by computers connected to the blockchain.



Smart contracts allow decentralized applications to connect to a blockchain. Decentralized apps (dApps) are like any web applications used – think Facebook – but give the developer the ability to use smart contracts on the platform. dApps can be extremely powerful tools that enable users more control over their personal data.

Blockchain has the potential to transform how personal data is collected, stored, shared, and managed. They allow trustless connections between two entities to take place, usually without the need for personal information. For example, blockchain technology may soon enable people – anywhere in the world – to obtain a loan they require without disclosing any personal information.

3 Building trust with blockchain

Blockchain is often referred to as a 'trustless network', not because you can't trust the people with whom you do business with; but because you don't have to when using a blockchain network.

Blockchain is able to build trust in a (business) network through the following four features:

- Distributed and sustainable: The ledger is shared and updated with every new transaction, and reproduced among all participants in near real time. The blockchain platform is independent of any single organization since it is not owned or controlled by anyone.
- Secure, private and permanent: Unauthorized access to the network is prevented by permissions and cryptography. This also ensures that participants are who they say they are. Confidentiality is maintained through cryptographic hashing. Participants cannot alter a transaction record once terms have been agreed upon; errors can only be corrected with new transactions.
- Transparent and auditable: Each party to a transaction has access to the same ledger, enabling them to validate transactions and establish ownership without the need for a third-party intermediaries. Transactions are time-stamped, chronologically ordered, and are validated in near real time.
- Consensus-based: Before a transaction can take place, all relevant network members must concur that the transaction is valid. This is obtained through the use of consensus algorithms. The conditions for a transaction or asset exchange can be established by each blockchain network.

4 Why blockchain can be important

A deeper understanding of blockchain can be obtained by investigating the environment in which it was created: the need for an efficient, affordable, trustworthy and secure system for carrying out and logging (financial) transactions.

Why blockchain?

Trust is an important part of any business transaction. In the past, people used minted coins, paper money, and letters of credit to establish trust between buyers and sellers. Today there are many innovations (like telephone lines, credit card systems, the Internet and mobile technologies) that can improve the speed, convenience and efficiency of transactions and meanwhile reduce the distance between buyers and sellers. However, many business interactions are still inefficient, expensive and vulnerable to fraud and cyber-attacks (especially centralized systems).

Global transaction volumes are increasing at an exponential rate, which will undoubtedly amplify the costs, vulnerabilities, inefficiencies, of transaction systems. This rise in transaction volumes has been driven by the evolution of e-commerce, online banking, IoT, and in-app purchases, as well as the growing mobility of individuals all over the world.

To tackle these challenges, the world requires quicker payment networks that establish trust, don't need specialized equipment, doesn't have recurring fees or chargebacks and provide a collective bookkeeping solution that guarantees transparency and trust. Bitcoin is one solution that's been developed to address these concerns.

Importance of blockchain

Business runs on information. The more accurate it is and the quicker it's received, the better. Because it offers immediate, distributed, and entirely transparent information kept on an immutable ledger, blockchain is perfect for delivering that information. Among other things, a blockchain network can track orders, payments and accounts. And because every member share the same version of the truth, everyone can see each detail of a transaction, increasing the confidence, as well as providing new efficiencies and opportunities. Thanks to the blockchain architecture, participants are able to share a ledger that is updated through peer-to-peer replication each time a transaction takes place. Peer-to-peer replication means that every participant (a node) in the network acts as both a publisher and a receiver. Each node has the ability to send and receive transactions to other nodes, and as the data is transferred, the data is synchronized across the network.

The blockchain network is efficient and cost-efficient because it eliminates duplication of effort and lowers the need for intermediaries. Because it uses consensus models to verify information, It's also less vulnerable. Transactions are protected, authenticated and validated.

The participants in both the traditional transaction systems and in a blockchain network are the same. What has changed is that the transaction record is now shared and available to all parties instead of being kept in a central database.

5 Blockchain governance

Blockchain governance can be regarded as the integration of norms and culture, the laws and the code, the people and the institutions that facilitate coordination and together determine a given organization (Fischer & Valiente, 2021).

Blockchains are neither sovereign states nor are they conventional multinational corporations with shareholders. No, blockchains are vast ecosystems of equally powerful actors working towards a common good.

These actors may fill different roles, such as developers, stake pool operators, enterprises, or general users. But ultimately, they all have a stake in what happens within the blockchain ecosystem. Each participant also has unique perspectives to offer.

Blockchain governance has, however, frequently had trouble encouraging community involvement while also working to benefit the larger ecosystem. In the past, it has also been challenging to make sure that individuals in charge of a community and those who push protocol changes remain representative of the community's overall viewpoints. The basic principles of blockchain governance across numerous distinct protocols have placed a strong emphasis on these challenges.

To address this, researchers have experimented with two main types of blockchain governance, both on-chain or off-chain. Let's take a look at how they differ:

On-chain Governance — As the name implies, on-chain governance uses voting methods on the blockchain, typically through tokens that represent stake and grant voting rights.

On-chain governance enables a wide range of ecosystem members to vote and have their opinions heard on important blockchain proposals and treasury decisions. It is theoretically designed to be genuinely decentralized.

Off-chain Governance — Off-chain governance does not use voting mechanisms based on the blockchain. As a result, token holders don't use their voting privileges to decide on proposals. Before recommendations are sent to a final board, or editors, who will supervise their implementation, there might still be a significant amount of community consensus on such recommendations.
It's likely that both on-chain governance and off-chain governance will be necessary for a fully functional blockchain ecosystem.

6 (Dis)advantages of blockchain

Advantages

The main advantages of blockchain have been described above in detail, but let's list them again for an overview. The main feature of blockchain is decentralization where there is no other instance required to act as an intermediary, reducing transaction validation times.

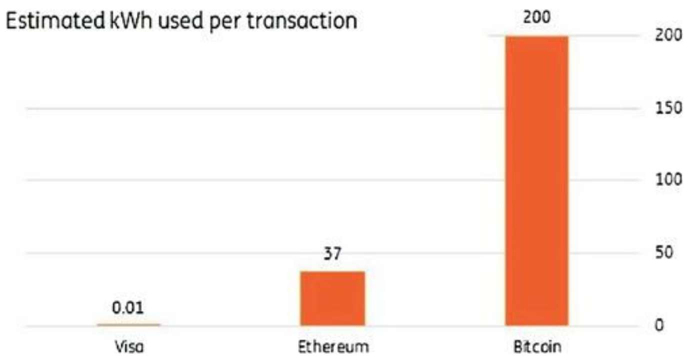
This also reduces cost of users. The next big advantage is network distribution, no one owns the network, allowing different users to always have multiple copies of the same information. Also, this feature makes it resistant and resilient to any type of failure because the fact that a node fails does not mean the network in general fails. Moreover, having a distributed network means that there are practically no errors because the information must be verified by many participants in the network. Incorrect or malicious information within the blockchain becomes practically impossible.

The reliability and transparency mentioned above are of course also big advantages of blockchain systems.

Disadvantages

As mentioned above, blockchain tech represents low costs for users, unfortunately, it also entails high implementation costs for companies which may delay its mass adoption.

While blockchain makes peer-to-peer transaction very efficient, it is inefficient to have several nodes verifying the same operations, since only one person will receive the reward from the mining process. If we take Bitcoin for example; it uses the Proof-of-Work consensus algorithm that relies on the miners to do the hard work. The miners have to solve complex mathematical problems. The high energy consumption is what makes these complex mathematical problems not so ideal for real word use. Every time the ledger is updated with a new transaction, the miners need to solve these problems which means spending a lot of energy. However not all blockchain solutions work in this manner. There are other consensus algorithms that have solved this problem. For example, permissioned or private networks do not have these problems as the number of nodes within the network is limited. Also, as there is no need for global consensus, they use efficient methods to reach consensus. There are also newer blockchain solutions that offer better solutions compared to the first generation of blockchain technology. Ethereum for example solved many inefficiencies by shifting to a better blockchain technology solution where there is a way of automation using smart contracts. It also adopted Proof-of-Stake (PoS) which is more efficient than that of Proof-of-Work (PoW).



An even newer blockchain called Solana uses Proof-of-History (a clock before consensus) which is very energy efficient *(An average Solana transaction consumes 2707 Joules of energy, less than three Google searches. In terms of crypto, while one Bitcoin transaction consumes 6,995,592,000 Joules of energy, and a single Ethereum transaction gobbles 692,820,000 Joules, https://solana.com/news/solanas-energy-use-report-march-2022)*

In short, permissioned networks are efficient when it comes to energy consumption whereas public networks can consume a lot of energy to remain operational.

Another possible bottleneck in blockchain tech is storage. As the number of users grows, the number of transactions that needs to be integrated into the blocks will also grow, so the storage capacity required will also have to increase inside the (miners') computers, eventually exceeding the capacity of hard disks. Clearly, there needs to be a better way to handle this as whenever the data is updated, nodes need to replicate it. Moreover, the size of the blockchain grows with more transactions and nodes. If it continues to grow, the whole network could be possibly slowed down, which is not ideal for commercial blockchains. Luckily, inefficiencies are slowly being improved with the help of cloud/storage solutions developed by Google, Amazon, Microsoft… But also other blockchain projects offer solutions like Arweave, Filecoin, GenesysGo (shadow drive). They are building decentralized storage protocols and even decentralized cloud solutions.

Another disadvantage that limits blockchain technology is interoperability. As mentioned above, there are multiple types of blockchain networks of which many work differently, all trying to develop a DLT-solution in their own unique way. This can lead to interoperability issues where these different chains are not able to communicate efficiently. As for the storage problem, there are projects out there that try to solve the interoperability issue (Quant Network for example).

This interoperability issue is also present in traditional transaction systems.

Finally, scalability is still an issue. The more people that participate in the network, the chances of the network slowing down are higher. For example, there has been some improving changes in blockchain technology. Some scalability options are being integrated with the Bitcoin network as well. A potential solution can be to do transactions off the blockchain and only use the blockchain to store and access the transaction information. However, most of these solutions are still not at the level of the centralized systems. When we compare the transaction speed of Bitcoin and VISA, we still see a huge difference between them. At this moment, Bitcoin can only process 7 transactions per second. In comparison, VISA can do 1700 transactions per second. Ethereum was doing about 20 transactions per second at the time of writing. Solana on the other hand can handle way more transactions per second - at the time of writing the tps was ± 3334 with an average cost of $0.00025 per transaction - which means it's much faster than VISA.

A two-edged sword

The immutable character of information stored on the blockchain can be seen as both an advantage and a disadvantage. It's clear that several systems benefit from it including supply chain, financial systems… But once data is written, it cannot be removed. If an error is recorded in the blockchain, it can't be removed.

Although for many users, anonymity, derived from the trust they have in blockchain technology for P2P transactions, is a virtue. Since this feature makes it practically impossible to track transactions, it has been used for illegal crimes.

To ensure blockchain is decentralized, it's crucial to give individual network participants the ability to act as their own bank. This can cause some other problems. To access the assets stored by the user on the blockchain, they need private keys. These are generated when a wallet is created, and it is the responsibility of the user to remember them or write them down and save them somewhere safe. They also can't share these keys with anyone else. As has been documented on many occasions, having lost them it becomes almost impossible to recover these keys

Blockchain is a disruptive technology that is still in a process of constant transformation and adaptation and therefore, during this development, it continues and will continue to present different challenges. It's important to be aware of the advantages and disadvantages mentioned above before we support massive adoption of blockchain technology.

7 NFTs

A specific application of blockchain that is getting a lot of attention lately is NFTs.

An NFT is a Non-Fungible Token or a unique digital identifier: an irreplaceable, non-exchangeable digital certificate of ownership, a digital claim to a unique piece of blockchain. Bitcoin for example is just like the euro or dollar fungible. It's a currency and it doesn't matter which bitcoin or euro you exchange; 1 bitcoin remains 1 bitcoin and is worth the same amount. An NFT is unique, and its value depends on several factors.

This certificate can be created digitally and linked to a digital object (e.g., an image) and that is then registered into a blockchain. This registration is linked to a digital crypto wallet. The person who created or bought the NFT then has a digital key in his/her wallet with which he/she can prove that the NFT is his/her property. Anyone around the world can see that person is the owner because the NFT is in the public blockchain, but no one can change the registration.

In short, an NFT is your own unique proof of ownership, authenticity and provenance. An NFT can be used as a means of transferring ownership. Thereby, every transaction is a "purchase agreement". Ownership of the NFT is then transferred, but the NFT itself is not an IP (Intellectual Property) right. With copyright, the creator of a work is the owner of the copyright to that particular right. When someone buys an NFT, that person acquires the beneficial ownership of the NFT and not the copyright to the work. Using smart contracts, however, it is possible to sell copyright along with ownership. This must then be explicitly programmed into the smart contract.

Applications in the agri-food sector?

Because of the ease with which agro-data can be replicated, it is difficult to trust a promise by an agri-tech company to respect farmers' ownership rights to their data. But if the agri-tech company links an NFT to a specific dataset uploaded to its servers, and then transfers that NFT to the farmer who generated the data, that company can essentially create a single, original dataset. Any subsequent copy, without the permission of the NFT owner or without transferring the NFT to the next user, could violate that owner's rights.

If data is the new oil, (corporate) NFTs are the tankers

Like oil, data can be extracted and refined - but how can data be transported to where it is needed most?

There is tremendous value to be realized by treating data as an asset, but this comes with challenges. Non-fungible tokens (NFTs) are one way to overcome these technological, regulatory and incentive-related barriers. While data and data analytics are important, many companies are becoming increasingly disillusioned with their attempts to extract value from them. What they are missing: sustainable value creation is possible when data is shared - not only within a company, but also across company boundaries, to gain insights and train artificial intelligence (AI) algorithms effectively.

In most cases, the problem is that each company has the data but does not or cannot share it with others in the ecosystem. Without a digital ecosystem for B2B data exchange, data is like oil; it can be extracted and refined, but it cannot be transported to where it is needed most

8 Decentralize DjustConnect?

The European agricultural sector has created a code of conduct on data sharing and especially on the support for the use of this data. All stakeholders sponsor and promote EUCoC4DS as the basis for sharing data, but another sharing initiative, called DjustConnect,

ensures that farmers have full control of their data. The NextDE Project, with its results, aims to contribute to the development of an Agricultural EU-US Data Sharing Network that targets a FAIR data economy supported by NGI technologies and decentralized architectures and systems. The primary goal is to develop and test a new business process to support the establishment of verified smart data-sharing contracts between data providers and consumers. This business process relied on blockchain technology and adopted a distributed architecture model to store the API contracts. DjustConnect (EU) was one of the primary technology actors. The platform DjustConnect is a public-private co-operation run by ILVO that provides data sharing services. DjustConnect aims to be a 'data highway', they provide a digital infrastructure for the secure exchange of data. EV ILVO is planning to integrate the identification and smart contracting technology as new services in the platform.
Since intermediary platforms like DjustConnect use centralized architecture models, they act as master nodes on these data networks. Consequently, they impose the participants' roles, responsibilities, and rights to support platform business models using constitutive agreements.

A smart contract template was developed. It can support the establishment of automated data-sharing agreements within a FAIR Data Economy. A formula that estimates the base price of an API resource was also produced. In the experiment a new service for the DjustConnect platform was started that will allow data partners of the platform, to negotiate on the API prices using estimated base prices, sign data-sharing contracts and store critical (agreement) information on a blockchain ledger. This new service will allow partners of the platform to complete the data only when negotiating parties have come to fair price agreements.

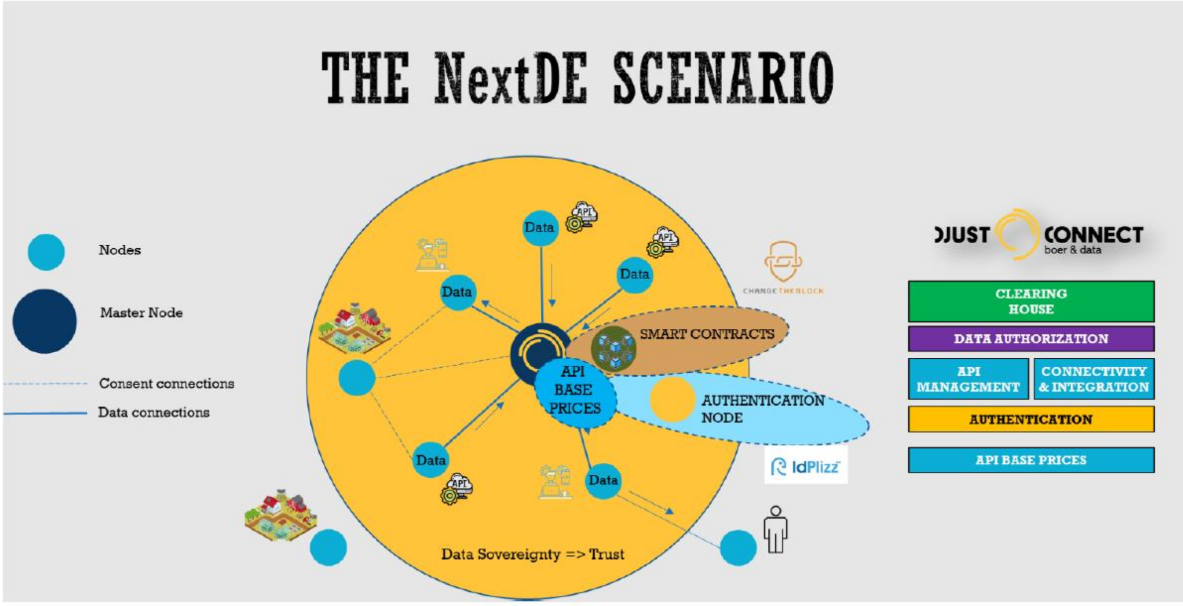
The adoption of a more decentralized model (like smart contracts and biometric identification) by DjustConnect and other intermediary platforms can:

- Better support the scale-up of the data economy network
- Increase the ability to perform cross-border transactions (EU-US e.g.)
- Support the further automation of data sharing as a way to achieve environmental, economic and social impact in the Agrifood sector
- Increase the participation of actors like technology services providers.
- Finally, it can also support the establishment of verified data sharing agreements and generate a low entry-level in a data sharing network.

DjustConnect stakeholders believe that a service like this can support the establishment of data access and usage agreements, further support technical and organizational/legal enforcement, and tackle two main obstacles:

a) The first one is related to the current lack of trust and transparency. Data providers ask, "How am I sure that the data consumer will use my data as he promised to do? What should I do to protect my data". Additionally, the farmers want to deliver their consent and be aware of the agreement's content between the provider and the consumer.

b) The second one is related to the lack of awareness or knowledge of the actual value of the API resources. For example, the providers ask, "What is an appropriate price for my API?", "Should I ask the same price if the usage period is one year or three years?" or "Should I ask for more when the conditions look favorable, or I should retain the price and keep it irrelevant to the data consumer?"



The main idea of the possible new, decentralized, version of DjustConnect, will be implementing the smart contracts module into the DjustConnect platform, where users from anywhere in the world will be able to sign contracts in a transparent, decentralized and intuitive way. The users will only need to connect to one platform to get all benefits from blockchain technology and a decentralized database. To increase the number of contracts within the platform, an API infrastructure where different developers can program their apps reliably and securely, can be opened. This will ensure protection of the data while promoting the creation of new ways of using it.
To ensure the reliability of the data, a shared connection for the database could be implemented. This kind of system allows different databases to be shared between several nodes, ensuring that no single person has access to the data, reducing possible cyber-attacks. This system will also improve data privacy.
The idea to decentralize DjustConnect seems very interesting for expanding the platform, but the NextDE project found that there are still too many technical and even more legal issues to overcome to build a decentralized data-sharing platform.

9 MIDIH & BOOST 4.0

MIDIH project

MIDIH (Manufacturing Industry Digital Innovation Hubs) MIDIH is a 'one-stop-shop' of services, offering industry access to advanced digital solutions, state-of-the-art industrial experiments, pools of human and industrial competencies. The European project is testing the use of distributed ledgers to track transactions between different stakeholders in different smart supply chain scenarios. It was found that there is a need for track and trace solutions that allow stakeholders to validate a product at different points throughout the supply chain. Blockchain technology has the potential to transform the supply chain by adding transparency, traceability and security to the supply chain (*https://www.bdva.eu/sites/default/files/BDVA_SMI_Discussion_Paper_Web_Version.pdf*).

To achieve a traceable and reliable supply chain, the supply chain must meet the increasing demand for origin information and there must be uniformity and compliance across sectors. New technologies like blockchain and *Industrial Data Spaces* (IDS) can play a crucial role in this. Blockchain can provide a holistic and secure tracking by providing consumers with trust in terms of origin, production conditions, specifications, producers, environmental safety, authenticity, etc. of a given product. The IDS-technologies (like definition and enforcement of usage policies) can provide protection of data sovereignty and trust in supply chains, e.g. the 'SICK' use case: *https://internationaldataspaces.org/usecases/SICK/*. Improving traceability can reduce the cost of quality problems, and increased trust creates a better environment for maintaining supply chain relationships and reduced risk and uncertainty.

With this blockchain and IDS-technology, reliable and secure data exchange becomes a very real possibility. Moreover, blockchain tech ensures responsiveness and accountability of transactions in data exchange between production equipment. *(https://midih.eu/documents/papers/BDVA_paper1.pdf)*

Some more interesting information:

https://www.iosb.fraunhofer.de/en/projects-and-products/indaspaceplus-industrial-data-spaces-plus.html

https://midih.eu/

https://internationaldataspaces.org/

Open source code IDS: *https://github.com/International-Data-Spaces-Association/idsa*

Boost 4.0 (Big Data for Factories)

Boost 4.0 (*Big Data Value Spaces for Competitiveness of European Connected Smart Factories 4.0*), launched in January 2018, is the largest European initiative in *Big Data for Industry 4.0*. The project aims to lead the construction of the *European Industrial Data Space* to improve the competitiveness and guides the European manufacturing industry towards the introduction to Big Data in the factory by providing the industrial sector with the necessary tools to get the most out of data. Boost 4.0 (Big Data for factories) has several main goals:

- Global standards
- Secure, digital infrastructures
- Trusted Big Data middleware
- Digital manufacturing platforms
- Certification

To this end, the project is rolling out the *Europese Industrial Data Space* and *Big Data Services* at 11 pilot factories (Volkswagen, Siemens, Philips…), evaluated in three strategic economic sectors (automotive, manufacturing equipment, household appliances). Each pilot has up to two scenarios with different processes being transformed using the Boost 4.0 initiative. In trial 1, for example, Volkswagen, ESI Group and ATB aim to develop a new approach to collect data from the molding process to understand, diagnose, predict and ultimately prescribe conditions for optimal overall efficiency. The Volkswagen pilot will implement a series of interconnected processes that should boost production efficiency, reduce costs and improve the quality of the metal to be molded.

Again, the major benefit of using blockchain is visibility and transparency of the manufacturing process to all parties in the business network, (re)traceability of parts and an irrefutable (manufacturing)process. Manufacturing networks take advantage of connectivity between customers, suppliers, manufacturers, partners and material things. They also cross geographical and regulatory boundaries. In today's manufacturing networks, each participant maintains its own ledger, which must be updated every time a transaction occurs. This is inefficient and expensive (https://boost40.eu/wp-content/uploads/2020/11/D2.3.pdf). Enter blockchain.

Blockchain

IBM is a partner in Boost 4.0 and is the leading provider of blockchain technology with more than 400 engagements worldwide. IBM is responsible within the project for applying blockchain in the use cases, leveraging Hyperledger Fabric, designed by Hyperledger Foundation (Linux Foundation) (https://www.hyperledger.org/). Hyperledger foundation is a non-profit organization that provides all the necessary resources and infrastructure to ensure thriving and stable ecosystems around open-source blockchain projects. Hyperledger Fabric (https://www.hyperledger.org/use/fabric) is an open source, permissioned (private) blockchain framework to support the development of blockchain based distributed ledgers. It provides a modular architecture with a delineation of roles between the nodes in the blockchain network, execution of smart contracts and configurable consensus and membership services. At the core of the framework is a distributed ledger that provides immutable recording of transactions taking place in the network. The Hyperledger Fabric infrastructure is built to offer a high degree of trust, resilience, flexibility and scalability (https://boost40.eu/wp-content/uploads/2020/11/D2.1.pdf). The platform allows all participating parties to share their data in a secure and controlled manner, managed by a consensus of all relevant parties. As previously mentioned in the general blockchain explanation above, each participant in the network has an immutable copy of the distributed data ledger, ensuring transparency, provenance,, increased trust and efficiency and reduced costs. All of this benefits data sovereignty. The big difference between Hyperledger Fabric and most other blockchain systems, is that it is private and permissioned. Not everyone has access to the network as is the case with e.g. Ethereum (see earlier).

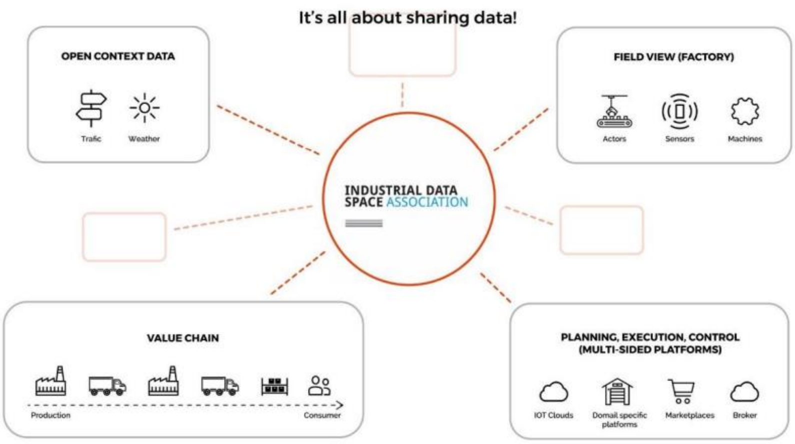
Data sovereignty in trusted data sharing remains one of the key industry challenges, especially in manufacturing when it comes to implementing advanced data value chains and realizing data-driven business models and operations. Boost 4.0 represents a joint effort with the entire industry to establish the rules, standards and reference frameworks to help enable the following:

- The free exchange of data (as assets)
- The growth of a large Big Data market
- A data driven transformation of manufacturing capabilities
- The creation of a vibrant European big data-centric ecosystem in support of Industry 4.0

(European) Industrial Data Space ((E)IDS)

This project contributes to the ambition of providing the first version of a business reference architecture with a shared model; namely, the EIDS that will empower European industry with the digital capability to handle industrial data and build advanced analytical services with full sovereignty and control. FIWARE technology can be used to implement an IDS business architecture with Open Source Software (OSS) components. This approach is also preferred by the Hyperledger Fabric blockchain initiative to integrate distributed ledger functionalities into the IDS.

The EIDS creates an ecosystem, where data is no longer just a simple sequence of numbers and letters, but where data constitutes a tradable/economic good that has a specific value.



To build such an ecosystem, two things are required:

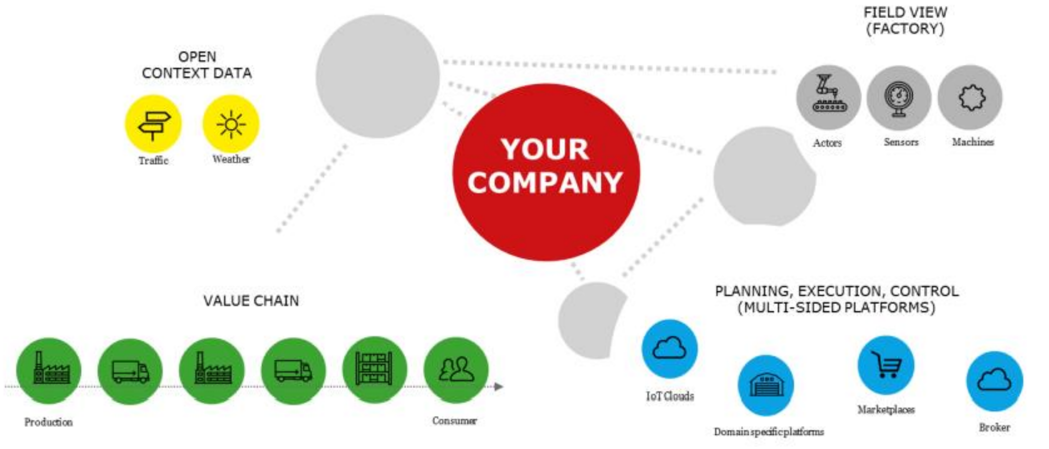
- huge numbers of sources of raw data
- *Big Data* applications, adding value to the raw data

There is also a need to make these sources of data easily accessible and the owners of this data must be promised that the data will be used only as authorized by them. There is a need for trust between the various participants of the EIDS. Therefore, the foundations of the EIDS is based on the architecture of the IDS. (EIDS serves the specific needs of the Big Data community and IDS is a domain-agnostic standard).

The IDS(A) (International Data Space Association) is an organization with nearly 100 members from all different types of industries and sizes. The goal of the IDS is to develop a global standard for the exchange of data. The continually growing volume and the rise of the data economy require standards that ensure the sovereignty of data. This is what the "IDS standard" will deliver, by defining an architecture for an entirely new ecosystem, enabling the exchange of data in a secure and sovereign manner in a trusted environment.

With technological evolutions (IoT, RFID...) and increasingly intensive data sharing between different players throughout the supply chain, there is a need for a way to share data, where the data producer retains full sovereignty over the data flow. This is what the IDS ecosystem stands for. Data sovereignty is the basis for trust between partners in the ecosystem. It is the ability of an individual or legal entity to decide exclusively and sovereignly on the use of data as an economic asset. Data sovereignty is about ownership, security and the value of data on the one hand, and about interoperability, data exchange, the "sharing economy" and data-centric services on the other. Today, there are still many obstacles to extensive data sharing. About half of companies are worried about inadvertently divulging valuable data or business secrets and are leery of losing control of their data. They also see inconsistent processes and systems as a major obstacle. About a third fear that platforms do not reach critical mass, so data exchange is not really interesting (https://www.pwc.de/en/digitale-transformation/data-exchange-as-a-first-step-towards-data-economy.pdf).

IDS brings improvements in terms of these obstacles, e.g., data security is assured, sovereignty is improved, and processes and cost structures are optimized. IDS can also provide further access to untapped data treasures in enterprises while maintaining control over data flow and use. This is achieved, among other things, by making data available, by linking with partners in the ecosystem, by controlling access to data (through usage control) and by creating value (e.g., by implementing apps). The image below shows an



overview of the IDS ecosystem.

This procedure works equally well for all industries and sectors. It provides self-determined control of data flows and leads to the following characteristics:

- Endless connectivity: IDS is a standard for data flows between all types of data endpoints
- Trust between different security domains. IDS provides comprehensive security features, providing a maximum level of trust.
- Governance for the data economy. IDS implements usage control and enforcement for data flows.

IDS is actually a peer-to-peer network of industrial data. All actors commit themselves to play by the rules of IDS. To ensure that all actors and components follow the rules, they must be certified by a trusted authority. All this gives the IDS architecture the following characteristics:

- Scaled-up economies due to network effects
- Open approach due to IDS being neutral and user-driven
- Trust by requiring all participants to be certified
- Decentralized approach due to distributed architecture
- Sovereignty over data and services
- Data governance imposes the rules
- Network platforms and services

FIWARE components can also contribute to a secure, reliable data exchange.

The use of IDS architecture, IBM Hyperledger Fabric and FIWARE connectors can enable the development of data-driven, secure and new services for a European data marketplace. By using the above technologies and tools of the BOOST 4.0 platform, the data analysis services developed will rely on security, data sovereignty and standardized interoperability.

As found in NextDE, this project also confirms that there are still many challenges on both the technical (e.g., the scalability and latency of blockchain-based smart contracts) and legal (currently no regulations regarding smart contracts) fronts.

https://boost40.eu/wp-content/uploads/2020/11/D3.1.pdf

10 Conclusion

Blockchain is able to ensure the integrity of data in data sharing, but as found in several EU project mentioned above, there are still many technical and legal challenges to overcome before blockchain can be used as a mainstream platform to share data. At the moment blockchain can be used to record transactions, but there are many projects trying to tackle the technical challenges and bring new utility to blockchain.

11 References

Fischer, A. & Valiente, M.-C. (2021). Blockchain governance. Internet Policy Review, 10(2).

https://forum.cardano.org/t/an-introduction-to-decentralized-governance-on-cardano/44590

https://iapp.org/news/a/the-promise-of-blockchain-in-the-digital-age-part-1/

http://www.giftbit.nl/tag/blockchain/

https://builtin.com/blockchain

https://www.ibm.com/blockchain/solutions/food-trust

https://www.researchgate.net/profile/Jon-Truby/publication/326603680_Decarbonizing_Bitcoin_Law_and_policy_choices_for_reducing_the_energy_consumption_of_Blockchain_technologies_and_digital_currencies/links/5d22f569a6fdcc2462ca9aba/Decarbonizing-Bitcoin-Law-and-policy-choices-for-reducing-the-energy-consumption-of-Blockchain-technologies-and-digital-currencies.pdf

https://www.rabobank.nl/bedrijven/groei/marktontwikkeling/vier-voordelen-van-blockchain

https://heinonline.org/HOL/LandingPage?handle=hein.journals/nyulpp18&div=34&id=&page

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

https://oceanprotocol.com/

https://ethereum.org/en/web3/

https://ec.europa.eu/newsroom/cef/items/760180/en

https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi

https://www.freecodecamp.org/news/what-is-web3/

https://doi.org/10.14763/2021.2.1554

(https://policyreview.info/glossary/blockchain-governance) https://www.jpmorganchase.com/news-stories/could-blockchain-have-great-impact-as-internet

https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/About+us

https://builtin.com/blockchain#:~:text=Blockchain%20Meaning%3A%20Blockchain%20Explained,distributed%2C%20not%20copied%20or%20transferred.

https://www.synopsys.com/glossary/what-is-blockchain.html

https://www.ibm.com/topics/what-is-blockchain

https://thunderbird.asu.edu/thought-leadership/insights/blockchain-business-beyond-crypto-and-bitcoin#:~:text=Blockchain%3A%20Each%20block%20is%20connected,inserted%20between%20two%20existing%20blocks.

https://andersbrownworth.com/blockchain/

https://therodmanlawgroup.com/distributed-ledger-technology/

https://medium.com/coinmonks/decoupling-blockchain-a8cb75759593