SMARTER

EXPERIENTIAL LEARNING TOOLS

Blockchain and smart contracts in smart supply chains

2022-1-FI01-KA220-HED-000086152

Co-funded by the Erasmus+ Programme of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Index

Introduction 2

Smart supply chains 4

Blockchain 6

How does the Blockchain work? 8

What is the consensus algorithm in Blockchain? 9

Smart contracts 10

How do smart contracts work? 12

Smart contracts and their benefits in the enterprise 13

References 14

Introduction

Blockchain is a technology that allows recording facts or events. Man's interest in recording facts is not recent, as we can go back to approximately 3200 B.C. to find the first record of data storage in single-entry records, what we understand today as databases, at which time it can be said that the systematic recording of information began. Some four thousand seven hundred years later, specifically in the year 1494 A.D., another historical milestone was reached when the first codified double-entry accounting system was created, inscribed in a mathematical book published in Venice.

The way of recording events and the technology used for this purpose evolved exponentially from the second half of the 20th century with the emergence of information technology. Until, from about 1991 onwards, and due to the rapid growth of the Internet, different works on non-centralized solutions for electronic payments appeared, that is, solutions that do not depend on the intervention of any central supervisory entity (i.e., an intermediary). This is where the idea of what we know today as cryptocurrency was born, although it was not yet associated with any implementation of registers or blocks.

On the other hand, also in 1991 the first work on a secure blockchain was published since it used cryptography. This work evolved through various authors, such as the British Adam Back, who in 1997, after a long process of study, proposed Hashcash, a system that initially intended, by means of a hash block algorithm, to combat unwanted mail or spam and which later ended up being a monetary system that gave rise, about a year later, to B-Money and Bit Gold in which the resources provided by distributed digital networks were already being used, with skill and efficiency, to carry out monetary operations. Finally, in 1998, Wei Dai, a Chinese computer engineer, described a solution to the above, a decentralized system for electronic payments, but incorporating public key cryptography, which guarantees payment security.

This work, in turn, was developed by other authors until 2008, when the article defining the mechanism to implement the most famous digital currency, Bitcoin, was published under the pseudonym of Satoshi Nakamoto. This cryptocurrency is based on the use of the Blockchain to record transactions in a P2P network[1]. For this reason, Wei Dai is commonly known as the precursor of the Blockchain, and Satoshi Nakamoto, whose real identity is unknown (although there are so-called candidates, but no evidence) as the inventor of Bitcoin.

This is why the Blockchain is often referred to as the technology behind Bitcoin, as if it were its sole purpose. But the reality is that the Blockchain serves to support a wide variety of applications. Through the Blockchain, all kinds of multi-user technologies can be implemented, such as distributed network storage (P2P network). On the other hand, it also serves to realize applications that greatly accelerate its process through the elimination of intermediaries, such as Internet voting, smart contracts, or non-fungible tokens (NFT).

The main difference between the usual centralized computing and the Blockchain is the way data is handled. In centralized computing, data is stored on centralized servers and controlled by a centralized entity. In contrast, in the Blockchain, data is stored in a decentralized network and is controlled by the community of network users. This decentralization makes the Blockchain more resistant to attacks and fraud, as there is no central point of failure. In addition, it is important to note that the Blockchain is not only a technology for recording transactions but can also be used to execute smart contracts.

A smart contract is a computer program that directly and automatically controls the transfer of digital assets between the parties under certain conditions. A smart contract works in the same way as a traditional contract and, in addition, it is executed automatically. Smart contracts are programs that execute exactly as they have been set up (coded, programmed) by their creators. Just as a traditional contract is enforceable by law, smart contracts are enforceable by code.

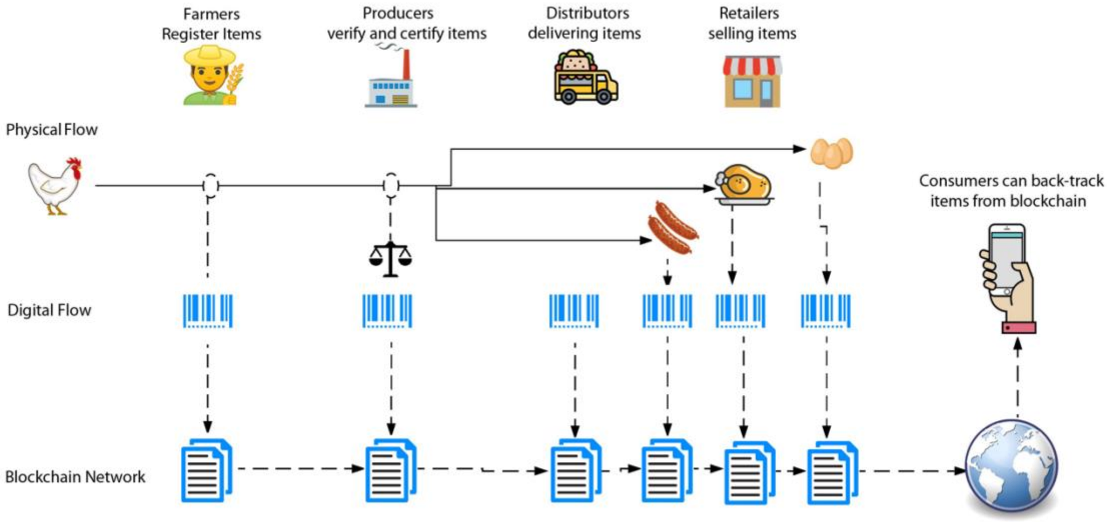
A smart contract employs basic conditions such as checking whether the amount of the asset value to be transferred is available in the sender's account. The Bitcoin network was the first to use some form of smart contract to transfer value from one person to another. Later the Ethereum platform emerged, considered

[1] A peer-to-peer network (P2P) network is a computer network in which all or some aspects operate without fixed clients or servers, but rather a series of nodes that behave as equals to each other. In other words, they act simultaneously as clients and servers with respect to the other nodes in the network. P2P networks allow the direct exchange of information, in any format, between the interconnected computers.

more powerful, precisely because developers/programmers could make custom contracts in a Turing-complete language[2]. It should be noted that the contracts written in the case of the Bitcoin network were written in a Turing-incomplete language, which restricted the potential for implementing smart contracts on the Bitcoin network. There are some common smart contract platforms like Ethereum, Solana, Polkadot, Hyperledger Fabric, etc.

Smart supply chains

More and more companies are operating on a global scale, which poses new challenges, especially in terms of risks of theft, efficiency, and traceability. Blockchain and smart contracts are technologies that can be used together to create a smart supply chain and avoid these risks. A smart supply chain is one that uses technology to automate and optimize processes along the entire supply chain, from raw material sourcing through manufacturing to delivery to the end consumer.

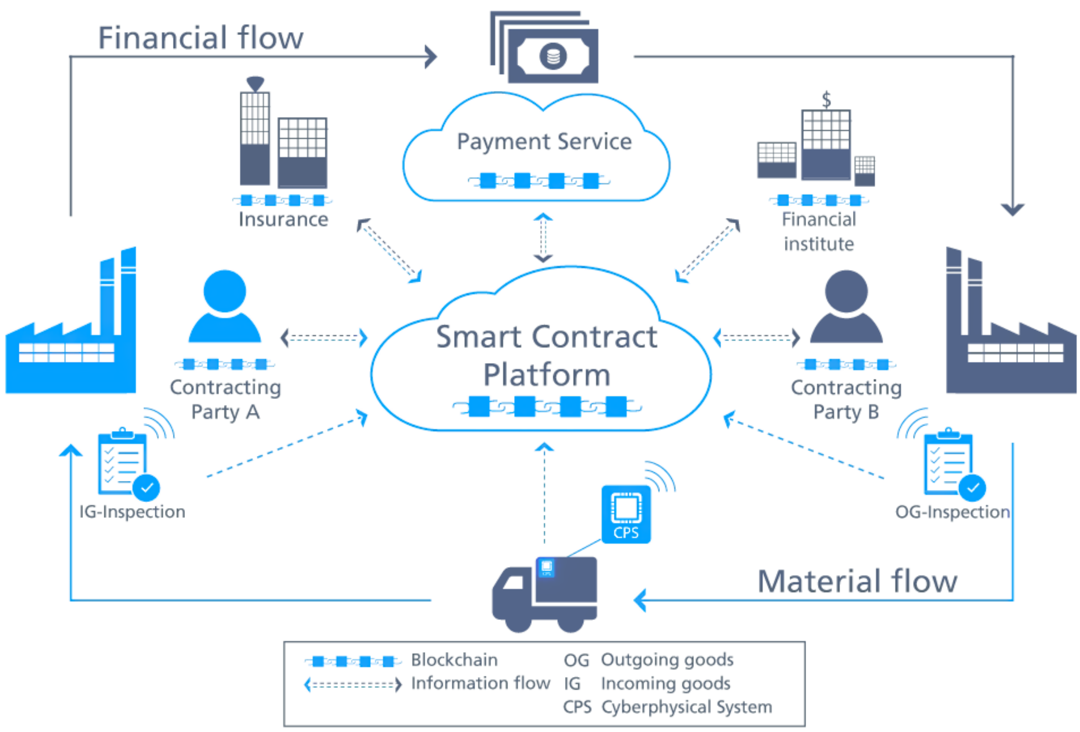


In a smart supply chain, the Blockchain can be used to track the end-to-end supply chain and provide transparency and security at every stage of the process. By recording every transaction on the Blockchain, all parties in the supply chain can have access to the same information, reducing errors and fraud. For example, if a product is manufactured in one country and shipped to another country for sale, the Blockchain can record every stage of the process, from manufacturing to delivery to the retailer. This can include information about the raw material supplier, the manufacturer, the transporter, the warehouseman and

[2] By Turing-complete we mean a language that has a computational capacity equivalent to what is called the Universal Turing Machine. In other words, Alan Turing devised a system that in theory could perform any type of calculation if unlimited physical resources were available. Applied to Blockchain technology and fundamentally to smart contracts, this concept refers to the ability of a language with this characteristic to be applied to solve any computational problem and implement complex structures such as loops.

the retailer. Each party in the supply chain can add information to the Blockchain, allowing all parties to have access to the same information. Companies can also use the Blockchain to improve the visibility of their supply chain by allowing all partners to post to a single ledger. This helps companies get a more accurate picture of where they stand and helps them improve and scale their core business processes. Even sensitive products such as food and pharmaceuticals can be distributed through a Blockchain platform, allowing customers to always buy authentic products and ensure that all parties comply with proper handling procedures.

On the other hand, smart contracts can be used in a smart supply chain to automate specific processes, such as payments, delivery registration, quality verification, among others. For example, if a retailer receives a shipment of products from a manufacturer, a smart contract can automate the payment process to the manufacturer once the retailer confirms that it has received the products in the established conditions. In addition, smart contracts can be programmed to trigger specific actions based on predefined conditions. For example, if a product does not meet agreed quality standards, the smart contract can trigger a specific action, such as sending an alert to the manufacturer so that the problem can be fixed.



Smart contracts connect the Blockchain to the real world and are critical to ensuring a more transparent and secure platform for conducting transactions. By using smart contracts, all types of transactions and services can be automated across the blockchain, providing several notable benefits such as automation, increased trust and security, elimination of intermediaries and facilitating quality control, among others.

However, despite the advantages of smart contracts in the supply chain, there are challenges that have arisen with their implementation, such as intolerance to errors, resistance to change, lack of standards and protocols, fear of privacy and differences in legislations.

Although Blockchain technology cannot eradicate all business problems, it can simplify many of the transactions that take place thanks to its central process of exchanging value and ownership.

In addition to offering advantages to companies, these technologies also benefit their customers. Smart contracts offer a credible customer-facing perspective and ensure the protection of information exchanged between parties. Blockchain can provide transparency and clarity to the entire supply chain, eliminating uncertainty and improving productivity. This would translate into a more effective distribution and improved selling experience for the company.

Blockchain

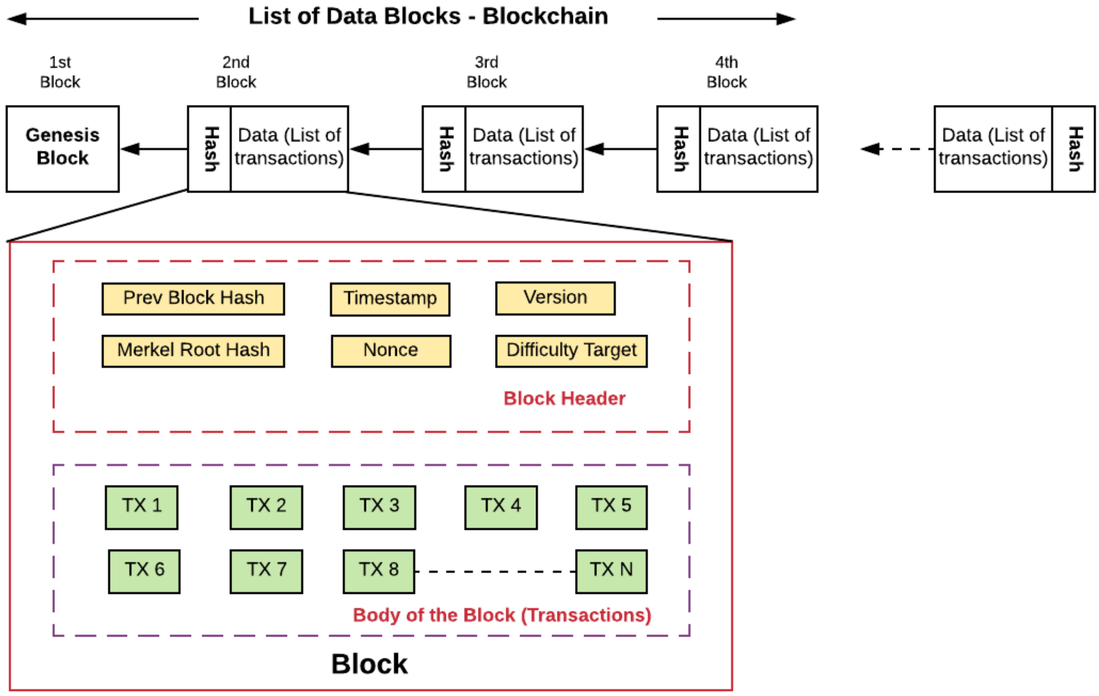
There are several definitions for what the Blockchain is, in a simple way we can define a Blockchain as a series of data structures, called blocks, which contain or record all the events that occur in a distributed system of a peer-to-peer network. Each block is connected to and depends on previous blocks that form a chain, the result is an "only attach at the end" system, i.e., a permanent and irreversible history that can be used as a real-time auditing system that allows any participant to verify the authenticity of each record simply by looking at the data itself.

Wikipedia defines it as: "*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. The timestamp proves that the transaction data existed when the block was created. 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 irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks*."

The Blockchain is a unique data structure that stores information in blocks, each containing a reference in the form of a hash[3] that points to the previous block.

[3] A sequence of bits obtained because of applying a cryptographic reduction function (also known as a hash function or digest function) on a finite sequence of input bytes. A hash function, h(x), must satisfy a number of properties: given an input *x* it must be easy and fast to compute *h(x)* but the input *x* must be very difficult (or impossible) to compute given *y=h(x)*. Furthermore it must be very difficult to find a pair *(x,y)* with *x≠y* such that *h(x)=h(y)*, i.e., that it is very difficult for collisions to occur. In general, these functions must be deterministic (a message always has the same hash value), computationally inexpensive (to be usable in practice),

This design ensures that the data in a block can only be modified by altering all subsequent blocks in the chain. This property provides the Blockchain with its fundamental characteristic: resistance to data modification. Thanks to this feature, the Blockchain can be utilized in distributed environments, forming a secure and immutable public database with irrefutable information. In essence, the Blockchain provides a tamper-proof platform for storing and sharing information that is both decentralized and transparent.



The Blockchain enables the maintenance of data integrity without the need for external means to centralize information. This is achieved by following a protocol order for all operations in which the chain participates. As a result, the Blockchain provides a secure and decentralized platform for storing and sharing information. Any potential attacker seeking to compromise the network would require a computing power greater than that of all the other nodes combined. In this way, the network remains secure and resilient against malicious attacks.

Formally, a Blockchain is a digital ledger that is publicly accessible, distributed, and decentralized. Its primary purpose is to store a record of transactions across multiple machines, which cannot be tampered with without network consensus. By using a peer-to-peer network with distributed timestamp servers, the information stored in this digital ledger can be verified and managed autonomously. The blocks that make up the Blockchain are validated or authenticated by users through a massive collaboration driven by personal interests, also known as miners. Unlike traditional digital content, the design of

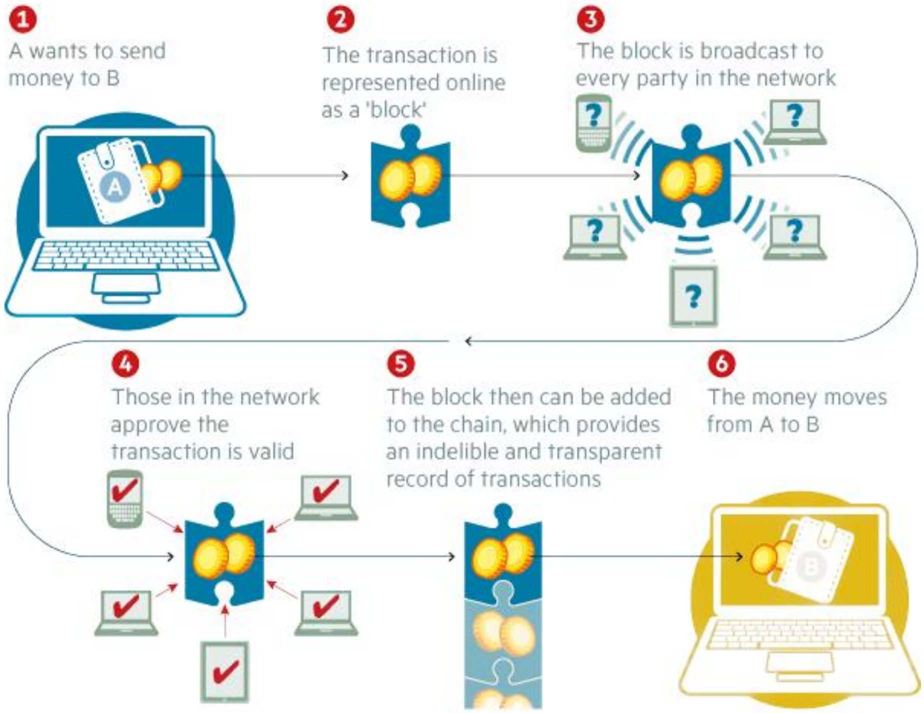
uniform and with avalanche effect with the goal that it is impossible to predict any hash value from other captured hash values.

the Blockchain ensures that transactions are unique and each monetary unit is transferred only once, thereby solving the problem of double-spending in digital currency. In essence, the Blockchain offers a reliable, tamper-proof platform for recording and verifying transactions that is both secure and decentralized.

In summary, Blockchain technology is an ideal solution for storing and organizing large amounts of data over time, while ensuring its authenticity and immutability. It is particularly well-suited for scenarios where data needs to be distributed across multiple nodes, rather than being held in a centralized system. One of the main advantages of Blockchain is its cost-effectiveness and efficiency, as it eliminates the need for intermediaries and reduces redundancy. Moreover, Blockchain is highly secure and tamper-proof, as it relies on consensus-based validation models to verify the accuracy of information. This results in transactions that are both authenticated and verifiable, making it a reliable and trustworthy platform for a variety of applications.

How does the Blockchain work?

To understand how Blockchain technology works, let's consider a hypothetical scenario involving two parties, A and B, who wish to transfer a digital currency or other asset. This transaction, along with other pending transactions, is compiled into a block and broadcasted to the network of computers participating in the Blockchain. These computers then validate the transaction in the block, based on agreed-upon rules and calculations through a consensus algorithm. Once a consensus is reached among most of the computers in the network, the transaction is considered verified and the block is assigned a unique hash code, as well as hash pointers to the preceding and succeeding blocks. This creates an immutable and secure chain of records. Finally, the value is transferred between the A and B accounts. At times, when validating multiple blocks simultaneously, chains of different lengths may be generated. In such cases, the solution to determining the correct string is typically to select the one with the longest length. The Blockchain thus provides a reliable, tamper-proof platform for recording and verifying transactions in a decentralized manner.



What is the consensus algorithm in Blockchain?

A consensus algorithm in Blockchain is a procedure that allows determining the validity of a transaction among the different nodes of the network, even if some of them have errors. In simple terms, it is a method for group decision-making. For example, suppose a group of ten people must decide on a win-win project. Each member can suggest an idea, but the majority must support the proposal that is most beneficial to the group as a whole. The others must accept that decision, whether they like it or not. Now imagine this same process with thousands of people, wouldn't it be more complicated? Consensus algorithms are not only based on most votes, but also seek an agreement that benefits all members of the network. Therefore, it is always a win for the network.

Some characteristics of this type of algorithms are:

- Reaching an agreement: The algorithm seeks to gather all possible agreements from the group.
- Collaboration: Each member of the network seeks the best agreement for the collective interests.
- Cooperation: All members of the network work as a team and put aside their own interests.
- Equal rights: All members of the network have the same value in voting, which means that every vote is important.
- Participation: All members of the network must participate in the voting, without exception.
- Activity: Each member of the network has equal responsibility and activity in the group.

The consensus algorithm used in the Blockchain is based on the Byzantine generals problem, which illustrates a war scenario involving a group of Byzantine generals who are besieging a city from different locations. To attack or retreat in a coordinated manner, the generals must agree on a course of action. However, only one general can issue the order, as he is the commander, while the rest are lieutenants.

The generals communicate through messengers, and the commander can issue one of two orders: "attack" or "retreat." The challenge arises when one or more of the generals may be traitors, whose goal is to cause disagreement among the loyal generals by providing false or misleading information. For instance, if the commander is a traitor, he may send contradictory orders to the lieutenants. If a lieutenant is a traitor, he may indicate to other lieutenants that the traitor is the commander, causing confusion among the group.

To solve the problem, we must look for algorithms that allow us to achieve one of the following objectives:

1. All loyal lieutenants make the same decision.
2. If the commander is loyal, then all loyal lieutenants carry out the order he decided.

The following additional conditions are usually considered in arriving at a solution:

1. Every message that is sent arrives correctly.
2. Each receiver of a message knows who is sending it.
3. The absence of a message can be detected.
4. In the absence of a message, you have a default order. This condition is to avoid the problem of the commander being a traitor and not sending orders.

The consensus algorithm in Blockchain technology generalizes this problem since there is usually no central node or commander to issue orders, and there is no hierarchical structure to obey them. Instead, the set of nodes must reach consensus. Proof-of-Work (PoW), Proof-of-Stake (PoS), and Proof-of-Authority (PoA) are among the most well-known types of consensus algorithms in Blockchain.

Smart contracts

Smart contracts are a cutting-edge technology that leverages the power of blockchain to automate the execution of contracts and agreements. In contrast to traditional contracts, which are typically based on legal documents and overseen by lawyers, smart contracts are self-executing computer programs that automatically carry out the terms of an agreement when specific pre-programmed conditions are met.

Smart contracts are a technology that can significantly reduce transaction costs by automating processes and eliminating intermediaries in commercial transactions. By doing so, they offer a more efficient and secure way of executing agreements. Moreover, smart contracts are based on Blockchain technology, which ensures transparency and immutability of the transactions recorded on the Blockchain. This makes the execution of agreements more secure, as any party can verify the transaction history and ensure that the contract has been executed according to the agreed terms. These are some of the capabilities of smart contracts:

- Accuracy: Smart contracts are executed with complete accuracy if the programmer has coded them correctly.
- Automation: Smart contracts can automate tasks that are normally done manually, reducing the possibility of errors and saving time.
- Speed: By automating tasks and eliminating the need for human interaction, smart contracts can be executed quickly, reducing the time required to complete transactions.
- Backup: Each node in a Blockchain maintains a shared ledger, which provides a reliable backup. This ensures that data is never lost or corrupted.
- Security: Smart contracts use cryptography to ensure the security of assets. Even if a hacker were to break the encryption, modifying all blocks after the modified block is very difficult and computationally intensive, making it virtually impossible for small to medium-sized organizations.
- Cost savings: Smart contracts eliminate intermediaries, reducing transaction costs. In addition, the minimal or no paperwork involved in smart contracts saves money.
- Information management: Smart contracts can manage user agreements and store information about an application, such as domain registration, membership records, etc.
- Multi-signature accounts: Smart contracts support multi-signature accounts, which distribute funds once all parties involved confirm the agreement, ensuring the security and reliability of transactions.
- Quality control: The Blockchain also ensures the provision of quality services and can serve as a platform to control and improve all activities carried out in the system.

Smart contracts have a wide range of applications across various industries. They are being increasingly used in sectors such as banking and finance, logistics, and supply chain management. In the banking and finance sector, smart contracts can automate lending processes and minimize the risks associated with fraud and errors. In the supply chain, they can be used to track products and automate payment and delivery processes, thereby increasing efficiency and reducing costs. Some essential features of a smart contract are as follows:

- Distributed: Everyone in the network has a copy of all the terms of the smart contract, and they cannot be changed by one of the parties. A smart contract is replicated and distributed to all nodes connected to the network.
- Deterministic: Smart contracts can only perform functions for which they were designed, only when the required conditions are met. The result will not vary, no matter who executes the smart contract.
- Immutable: Once deployed, a smart contract cannot be changed, it can only be removed if the functionality is previously implemented.
- Autonomy: No third parties are involved. The contract is created by a user and shared between the parties. There are no intermediaries involved,

which minimizes harassment and gives full authority to the contracting parties. In addition, the smart contract is maintained and executed by all nodes in the network, removing all power of control from any one party.
- Customizable: Smart contracts can be modified or customized before they are launched to do what the user wants them to do.
- Transparent: Smart contracts are always stored in a distributed public registry called blockchain, so the code is visible to everyone, whether they are participants in the smart contract.
- Reliability: Third parties are not required to verify the integrity of the process or to verify if the required conditions are met.
- Self-verification: Smart contracts are self-verifying due to automated capabilities.
- Self-executing: They are self-executing when the conditions and rules are fulfilled at all stages.

How do smart contracts work?

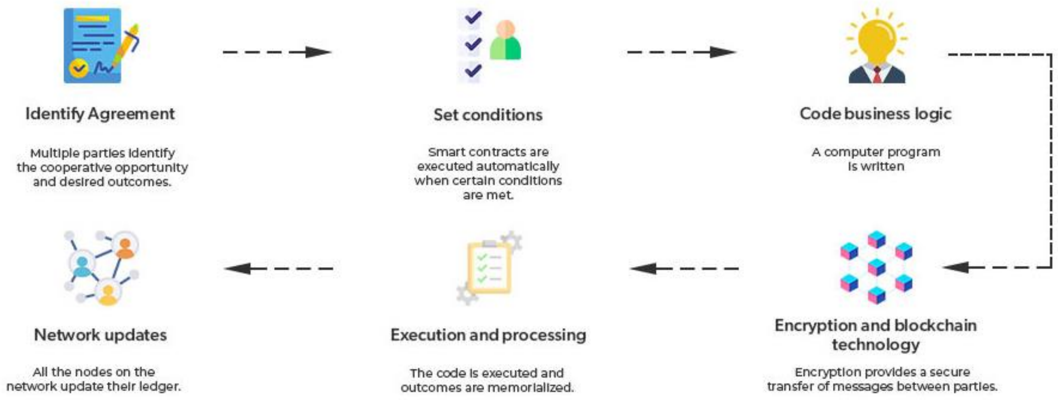
As we have seen, a smart contract is a digital version of a traditional contract that incorporates the security of the blockchain through its encryption, including details and permissions that are written in code and require an exact sequence of events to be fulfilled to trigger the agreed terms. Time constraints can also be set for contract fulfillment. In addition, each smart contract has its own address on the blockchain and can be interacted with through that address, provided the contract has been broadcast on the network.

The logic behind smart contracts is simple and is based on an IF-THEN structure, e.g. "IF you send object A, THEN the corresponding sum (in cryptocurrency or money) will be transferred to you", "IF you transfer a certain amount of digital assets, THEN object A will be transferred to you", or "IF I finish the job, THEN the agreed digital assets will be transferred to me".

It is important to note that the WHEN constraint can be added to include the time factor in smart contracts. Smart contracts allow setting precise conditions that must be met for the execution of the terms agreed upon in the contract. In addition, there is no limit on the number of IF or THEN conditions that can be included in a smart contract.

The process of executing a smart contract consists of the following stages:
- Defining the objective: First, the objective of the smart contract is defined. For example, a contract can be created to offer an IT solution to customers. All the terms of the contract are encoded and sent to the network.
- Reaching an agreement with the customer: once the contract is available on the network, all interested parties can discuss and evaluate the terms of the contract before reaching an agreement.
- Confirmation of the agreement: once an agreement is reached, both parties must use an electronic signature to confirm acceptance. Blockchain technology ensures that all contract requirements are met.

- Contract execution: once the agreement is confirmed, the transaction is executed, and the payment is sent to the recipient. Each transaction record is automatically created through the smart contract code. This process is repeated until all obligations stipulated in the contract have been successfully fulfilled.



Smart contracts and their benefits in the enterprise

The Blockchain together with smart contracts offer significant value to organizations, simplifying all operations and making transactions transparent and simple. All tasks are executed, controlled and recorded by the system, without parties being able to take actions behind the curtains.

With smart contracts, you can be sure that all parties will fulfill their commitments as agreed, eliminating legal errors, risks of manipulation and fraud. Everything is based on the principle of "if I do this, I get that", and "if I don't do this, I don't get that". Everyone is on equal footing, and it is impossible to cheat or spend bitcoin twice.

Among the benefits of smart contracts is automation, although it is not the only one, as smart contracts can also offer:

- Trust and transparency: Once deployed, neither party can change the terms of the contract for personal gain. In addition, all terms are visible to the parties, allowing them to follow the execution of the contract and review transaction information.
- Security: Each record is connected to the previous and next, making it difficult for hackers to change a single ledger record. In addition, although the records are accessible to anyone, the anonymity of the parties is maintained, as no names or private details are revealed.
- Automation: Standard contracts allow for the possibility of one or both parties cheating, ignoring certain aspects of the agreement, executing terms differently or not executing them at all. In contrast, the automation of smart contracts means that all the work is done mechanically without the need for any intermediaries. In addition, because everything is handled by software, cases of data falsification or non-compliance with any part of the contract are eliminated.

- Cost reduction: Through automation and encryption, entrepreneurs can significantly reduce operational costs. Accenture indicates that investment banks alone could save $8 billion a year by adopting smart contract technology. All transactions are fully visible to all parties involved, and multiple intermediaries are not required to make and monitor complicated payments. Instead, anyone can streamline all transactions themselves in real time, without having to pay fees, charges or commissions.
- Accuracy, efficiency and agility: Automation streamlines all the steps involved, ensuring accurate and efficient contract execution. As soon as the prerequisites are met, the required action is performed automatically, regardless of who is involved in the operation.

References

1. Adams, Colin. Estonia, A Blockchain Model for Other Countries. *Invest in Blockchain*. 2018. [Link]
2. Ante, L. Smart contracts on the blockchain–A bibliometric analysis and review. *Telemat. Inform.* 2021, *57*, 101519. [Link]
3. Bodó, B.; Gervais, D.; Quintais, J.P. Blockchain and smart contracts: The missing link in copyright licensing? *Int. J. Law Inf. Technol.* 2018, *26*, 311–336. [Link]
4. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* 2014, *3*, 2-1. [Link]
5. Chakraborty, P.; Shahriyar, R.; Iqbal, A.; Bosu, A. Understanding the software development practices of blockchain projects: A survey. In Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement; Computing Machinery: New York, NY, USA, 2018; pp. 1–10.
6. Chang, S.E.; Chen, Y.-C.; Lu, M.-F. Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technol. Forecast. Soc. Change* 2019, *144*, 1–11. [Link]
7. Davidson, S.; De Filippi, P.; Potts, J. Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. 2016. [Link]
8. De Giovanni, P. Blockchain and smart contracts in supply chain management: A game theoretic model. *Int. J. Prod. Econ.* 2020, *228*, 107855. [Link]
9. Destefanis, G.; Marchesi, M.; Ortu, M.; Tonelli, R.; Bracciali, A.; Hierons, R. Smart contracts vulnerabilities: A call for blockchain software engineering? In Proceedings of the 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Campobasso, Italy, 20 March 2018; pp. 19–25.
10. DreamzIoT. How Smart the Smart Contract in Helping the Supply Chain? [Link]
11. Dolgui, A.; Ivanov, D.; Potryasaev, S.; Sokolov, B.; Ivanova, M.; Werner, F. Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain. *Int. J. Prod. Res.* 2020, *58*, 2184–2199. [Link]
12. Eenmaa-Dimitrieva, H.; Schmidt-Kessen, M.J. Creating markets in no-trust environments: The law and economics of smart contracts. *Comput. Law Secur. Rev.* 2019, *35*, 69–88. [Link]
13. Ethereum Foundation. Ethereum: Blockchain Platform. [Link]
14. Fraunhofer ILM. Blockchain and Smart Contracts: Efficient and Secure Value Networks. [Link]
15. Feng, T.; Yu, X.; Chai, Y.; Liu, Y. Smart contract model for complex reality transaction. *Int. J. Crowd Sci.* 2019, *3*, 184–197. [Link]
16. Finck, M. Blockchains and data protection in the European Union. *Eur. Data Prot. L. Rev.* 2018, *4*, 17. [Link]
17. Goldenfein, J.; Leiter, A. Legal engineering on the blockchain:'Smart contracts' as legal conduct. *Law Crit.* 2018, *29*, 141–149. [Link]
18. Governatori, G.; Idelberger, F.; Milosevic, Z.; Riveret, R.; Sartor, G.; Xu, X. On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artif. Intell. Law* 2018, *26*, 377–409. [Link]
19. Greenspan, G. Smart Contracts: The Good, the Bad and the Lazy. 2015. [Link]
20. Hasan, H.R.; Salah, K. Proof of delivery of digital assets using blockchain and smart contracts. *IEEE Access* 2018, *6*, 65439–65448. [Link]
21. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* 2021, *177*, 102857. [Link]
22. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E.; Bani-Hani, A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer Peer Netw. Appl.* 2021, *14*, 2901–2925. [Link]
23. Li, Y.; Yang, W.; He, P.; Chen, C.; Wang, X. Design and management of a distributed hybrid energy system through smart contract and blockchain. *Appl. Energy* 2019, *248*, 390–405. [Link]

24. Lin, I-C, and T-C Liao. "A Survey of Blockchain Security Issues and Challenges." *IJ Network Security*. 2017, 19, 653-659.
25. Liebenau, J.; Elaluf-Calderwood, S. Blockchain Innovation beyond Bitcoin and Banking. 2016. [Link]
26. Macrinici, D.; Cartofeanu, C.; Gao, S. Smart contract applications within blockchain technology: A systematic mapping study. *Telemat. Inform.* 2018, *35*, 2337–2354. [Link]
27. Madanchian, M.; Taherdoost, H. The Impact of Digital Transformation Development on Organizational Change. In *Driving Transformative Change in E-Business through Applied Intelligence and Emerging Technologies*; IGI Global: Hershey, PA, USA, 2022; pp. 1–24.
28. Marino, B.; Juels, A. Setting standards for altering and undoing smart contracts. In *Rule Technologies. Research, Tools, and Applications*; Springer: Cham, Switzerland, 2016; pp. 151–166.
29. Namasudra, S.; Deka, G.C.; Johri, P.; Hosseinpour, M.; Gandomi, A.H. The revolution of blockchain: State-of-the-art and research challenges. *Arch. Comput. Methods Eng.* 2021, *28*, 1497–1515. [Link]
30. Nakamoto, S.; Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* 2008, 21260. [Link]
31. Oliva, G.A.; Hassan, A.E.; Jiang, Z.M.J. An exploratory study of smart contracts in the Ethereum blockchain platform. *Empir. Softw. Eng.* 2020, *25*, 1864–1904. [Link]
32. Ozelli, Selva. US Government Implements Blockchain Programs to Improve Transparency and Efficiency: Expert Blog. Cointelegraph: The future of money. 2018. [Link]
33. Panescu, A.-T.; Manta, V. Smart contracts for research data rights management over the ethereum blockchain network. *Sci. Technol. Libr.* 2018, *37*, 235–245. [Link]
34. Perera, S.; Nanayakkara, S.; Rodrigo, M.; Senaratne, S.; Weinand, R. Blockchain technology: Is it hype or real in the construction industry? *J. Ind. Inf. Integr.* 2020, *17*, 100125. [Link]
35. Ream, J.; Chu, Y.; Schatsky, D. Upgrading blockchains: Smart contract use cases in industry. *Retrieved Dec.* 2016, *12*, 2017.
36. Philipp, R.; Prause, G.; Gerlitz, L. Blockchain and smart contracts for entrepreneurial collaboration in maritime supply chains. *Transp. Telecommun.* 2019, *20*, 365–378. [Link]
37. Rouhani, S.; Deters, R. Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access* 2019, *7*, 50759–50779. [Link]
38. Sharma, P.; Jindal, R.; Borah, M.D. Blockchain-based decentralized architecture for cloud storage system. *J. Inf. Secur. Appl.* 2021, *62*, 102970. [Link]
39. Sklaroff, J.M. Smart contracts and the cost of inflexibility. *Univ. Pa. Law Rev.* 2017, *166*, 263.
40. Swan, M. *Blockchain: Blueprint for a New Economy*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
41. Szabo, N. The idea of smart contracts. *Nick Szabo's Pap. Concise Tutor.* 1997, *6*, 199.
42. Taherdoost, H.A. Critical Review of Blockchain Acceptance Models—Blockchain Technology Adoption Frameworks and Applications. *Computers* 2022, *11*, 24. [Link]
43. Vacca, A.; Di Sorbo, A.; Visaggio, C.A.; Canfora, G. A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. *J. Syst. Softw.* 2021, *174*, 110891. [Link]
44. Vaidya, Kiran. "The Byzantine Generals' Problem." Medium. [Link]
45. Vangala, A.; Sutrala, A.K.; Das, A.K.; Jo, M. Smart contract-based blockchain-envisioned authentication scheme for smart farming. *IEEE Internet Things J.* 2021, *8*, 10792–10806. [Link]
46. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.-Y. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Trans. Syst. Man Cybern. Syst.* 2019, *49*, 2266–2277. [Link]
47. Wang, Y.; He, J.; Zhu, N.; Yi, Y.; Zhang, Q.; Song, H.; Xue, R. Security enhancement technologies for smart contracts in the blockchain: A survey. *Trans. Emerg. Telecommun. Technol.* 2021, *32*, e4341. [Link]
48. Wüst, Karl and Arthur Gervais. "Do You Need a Blockchain?" *Proceedings of Crypto Valley Conference on Blockchain Technology*. 2018. [Link]
49. Xuan, S.; Zheng, L.; Chung, I.; Wang, W.; Man, D.; Du, X.; Yang, W.; Guizani, M. An incentive mechanism for data sharing based on blockchain with smart contracts. *Comput. Electr. Eng.* 2020, *83*, 106587. [Link]
50. Yuan, R.; Xia, Y.-B.; Chen, H.-B.; Zang, B.-Y.; Xie, J. Shadoweth: Private smart contract on public blockchain. *J. Comput. Sci. Technol.* 2018, *33*, 542–556. [Link]
51. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* 2020, *105*, 475–491. [Link]
52. Zou, W.; Lo, D.; Kochhar, P.S.; Le, X.-B.D.; Xia, X.; Feng, Y.; Chen, Z.; Xu, B. Smart contract development: Challenges and opportunities. *IEEE Trans. Softw. Eng.* 2019, *47*, 2084–2106. [Link]